Enterasys® SecureStack™ C3

Stackable Switches

Configuration Guide

Firmware Version 6.03.xx.xxxx

P/N 9034313-07

Notice

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810

Part Number: 9034313-07 June 2009

Documentation URL: http://www.enterasys.com/support/manuals

Documentacion URL: http://www.enterasys.com/support/manuals

Dokumentation im Internet: http://www.enterasys.com/support/manuals

Version:	Information in this guide refers to SecureStack C3 firmware version 6.03.xx.xxxx or higher.

Enterasys Networks, Inc. Firmware License Agreement

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement ("Agreement") between the end user ("You") and Enterasys Networks, Inc., on behalf of itself and its Affiliates (as hereinafter defined) ("Enterasys") that sets forth Your rights and obligations with respect to the Enterasys software program/firmware (including any accompanying documentation, hardware or media) ("Program") in the package and prevails over any additional, conflicting or inconsistent terms and conditions appearing on any purchase order or other document submitted by You. "Affiliate" means any person, partnership, corporation, limited liability company, other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. This Agreement constitutes the entire understanding between the parties, with respect to the subject matter of this Agreement. The Program may be contained in firmware, chips or other media.

BY INSTALLING OR OTHERWISE USING THE PROGRAM, YOU REPRESENT THAT YOU ARE AUTHORIZED TO ACCEPT THESE TERMS ON BEHALF OF THE END USER (IF THE END USER IS AN ENTITY ON WHOSE BEHALF YOU ARE AUTHORIZED TO ACT, "YOU" AND "YOUR" SHALL BE DEEMED TO REFER TO SUCH ENTITY) AND THAT YOU AGREE THAT YOU ARE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES, AMONG OTHER PROVISIONS, THE LICENSE, THE DISCLAIMER OF WARRANTY AND THE LIMITATION OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO ENTER INTO THIS AGREEMENT, ENTERASYS IS UNWILLING TO LICENSE THE PROGRAM TO YOU AND YOU AGREE TO RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, LEGAL DEPARTMENT AT (978) 684-1000.

You and Enterasys agree as follows:

1. LICENSE. You have the non-exclusive and non-transferable right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this Agreement.

2. RESTRICTIONS. Except as otherwise authorized in writing by Enterasys, You may not, nor may You permit any third party to:

(a) Reverse engineer, decompile, disassemble or modify the Program, in whole or in part, including for reasons of error correction or interoperability, except to the extent expressly permitted by applicable law and to the extent the parties shall not be permitted by that applicable law, such rights are expressly excluded. Information necessary to achieve interoperability or correct errors is available from Enterasys upon request and upon payment of Enterasys' applicable fee.

(b) Incorporate the Program in whole or in part, in any other product or create derivative works based on the Program, in whole or in part.

(c) Publish, disclose, copy reproduce or transmit the Program, in whole or in part.

(d) Assign, sell, license, sublicense, rent, lease, encumber by way of security interest, pledge or otherwise transfer the Program, in whole or in part.

(e) Remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Program.

3. APPLICABLE LAW. This Agreement shall be interpreted and governed under the laws and in the state and federal courts of the Commonwealth of Massachusetts without regard to its conflicts of laws provisions. You accept the personal jurisdiction and venue of the Commonwealth of Massachusetts courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

4. EXPORT RESTRICTIONS. You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Section 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Cambodia, Cuba, Georgia, Iraq, Kazakhstan, Laos, Libya, Macau, Moldova, Mongolia, North Korea, the People's Republic of China, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The enclosed Program (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Program is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

6. DISCLAIMER OF WARRANTY. EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED TO YOU IN WRITING BY ENTERASYS, ENTERASYS DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT WITH RESPECT TO THE PROGRAM. IF IMPLIED WARRANTIES MAY NOT BE DISCLAIMED BY APPLICABLE LAW, THEN ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THIRTY (30) DAYS AFTER DELIVERY OF THE PROGRAM TO YOU.

7. LIMITATION OF LIABILITY. IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS FOREGOING LIMITATION SHALL APPLY REGARDLESS OF THE CAUSE OF ACTION UNDER WHICH DAMAGES ARE SOUGHT.

THE CUMULATIVE LIABILITY OF ENTERASYS TO YOU FOR ALL CLAIMS RELATING TO THE PROGRAM, IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID TO ENTERASYS BY YOU FOR THE RIGHTS GRANTED HEREIN.

8. AUDIT RIGHTS. You hereby acknowledge that the intellectual property rights associated with the Program are of critical value to Enterasys, and, accordingly, You hereby agree to maintain complete books, records and accounts showing (i) license fees due and paid, and (ii) the use, copying and deployment of the Program. You also grant to Enterasys and its authorized representatives, upon reasonable notice, the right to audit and examine during Your normal business hours, Your books, records, accounts and hardware devices upon which the Program may be deployed to verify compliance with this Agreement, including the verification of the license fees due and paid Enterasys and the use, copying and deployment of the Program. Enterasys' right of examination shall be exercised reasonably, in good faith and in a manner calculated to not unreasonably interfere with Your business. In the event such audit discovers non-compliance with this Agreement, including copies of the Program made, used or deployed in breach of this Agreement, You shall promptly pay to Enterasys the appropriate license fees. Enterasys reserves the right, to be exercised in its sole discretion and without prior notice, to terminate this license, effective immediately, for failure to comply with this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

9. OWNERSHIP. This is a license agreement and not an agreement for sale. You acknowledge and agree that the Program constitutes trade secrets and/or copyrighted material of Enterasys and/or its suppliers. You agree to implement reasonable security measures to protect such trade secrets and copyrighted material. All right, title and interest in and to the Program shall remain with Enterasys and/or its suppliers. All rights not specifically granted to You shall be reserved to Enterasys.

10. ENFORCEMENT. You acknowledge and agree that any breach of Sections 2, 4, or 9 of this Agreement by You may cause Enterasys irreparable damage for which recovery of money damages would be inadequate, and that Enterasys may be entitled to seek timely injunctive relief to protect Enterasys' rights under this Agreement in addition to any and all remedies available at law.

11. ASSIGNMENT. You may not assign, transfer or sublicense this Agreement or any of Your rights or obligations under this Agreement, except that You may assign this Agreement to any person or entity which acquires substantially all of Your stock assets. Enterasys may assign this Agreement in its sole discretion. This Agreement shall be binding upon and inure to the benefit of the parties, their legal representatives, permitted transferees, successors and assigns as permitted by this Agreement. Any attempted assignment, transfer or sublicense in violation of the terms of this Agreement shall be void and a breach of this Agreement.

12. WAIVER. A waiver by Enterasys of a breach of any of the terms and conditions of this Agreement must be in writing and will not be construed as a waiver of any subsequent breach of such term or condition. Enterasys' failure to enforce a term upon Your breach of such term shall not be construed as a waiver of Your breach or prevent enforcement on any other occasion.

13. SEVERABILITY. In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired thereby, and that provision shall be reformed, construed and enforced to the maximum extent permissible. Any such invalidity, illegality, or unenforceability in any jurisdiction shall not invalidate or render illegal or unenforceable such provision in any other jurisdiction.

14. TERMINATION. Enterasys may terminate this Agreement immediately upon Your breach of any of the terms and conditions of this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

Contents

Chapter 4: Activating Licensed Features

Chapter 5: Configuring System Power and PoE

Chapter 6: Discovery Protocol Configuration

Chapter 7: Port Configuration

Chapter 8: SNMP Configuration

Chapter 9: Spanning Tree Configuration

Chapter 10: 802.1Q VLAN Configuration

Chapter 11: Policy Classification Configuration

Chapter 12: Port Priority Configuration

Chapter 13: IGMP Configuration

Chapter 14: Logging and Network Management

Chapter 15: RMON Configuration

Chapter 16: DHCP Server Configuration

Chapter 20: IPv4 Routing Protocol Configuration

Chapter 21: IPv6 Management

Chapter 22: IPv6 Configuration

Chapter 25: OSPFv3 Configuration

Chapter 26: Authentication and Authorization Configuration

Chapter 27: TACACS+ Configuration

Chapter 28: sFlow Configuration

Appendix A: Policy and Authentication Capacities

Index

Figures

Tables

About This Guide

Welcome to the *Enterasys® SecureStack™* C3 *Configuration Guide*. This manual explains how to access the device's Command Line Interface (CLI) and how to use it to configure SecureStack C3 switch devices.

Important Notice

Depending on the firmware version used in your C3 device, some features described in this document may not be supported. Refer to the Release Notes shipped with your device to determine which features are supported.

Using This Guide

A general working knowledge of basic network operations and an understanding of CLI management applications is helpful before configuring the SecureStack device.

This manual describes how to do the following:

- Access the SecureStack CLI.
- Use CLI commands to perform network management and device configuration operations
- Establish and manage Virtual Local Area Networks (VLANs).
- Establish and manage static and dynamically-assigned policy classifications.
- Establish and manage priority classification.
- Configure IP routing and routing protocols, including RIP versions 1 and 2, OSPF, DVMRP, IRDP, and VRRP.
- Configure IPv6 routing, including OSPFv3.
- Configure security protocols, including 802.1X and RADIUS, SSHv2, PWA, MAC locking, and MAC authentication.
- Configure access control lists (ACLs).

Structure of This Guide

The guide is organized as follows:

Chapter 1, **Introduction,** provides an overview of the tasks that can be accomplished using the CLI interface, an overview of local management requirements, an overview of the device's factory default settings, and information about using the Command Line Interface (CLI).

Chapter 2, **Configuring Switches in a Stack**, provides information about how to configure and manage stacked switches.

Chapter 3, **Basic Configuration**, provides how to set basic system properties, how to download a firmware image, how to configure WebView and Telnet, how to manage configuration files, how to set the login password, and how to exit the CLI.

Chapter 4, **Activating Licensed Features** describes the commands used to enable advanced routing and IPv6 routing licensed features.

Chapter 5, **Configuring System Power and PoE**, describes the commands used to review and set system power and PoE parameters on devices that offer Power over Ethernet.

Chapter 6, **Discovery Protocol Configuration** provides how to configure discovery protocols supported by the device.

Chapter 7, **Port Configuration**, describes how to review and configure console port settings, and how to enable or disable switch ports and configure switch port settings, including port speed, duplex mode, auto-negotiation, flow control, port mirroring, link aggegation and broadcast suppression.

Chapter 8, **SNMP Configuration**, describes how to configure SNMP users and user groups, access rights, target addresses, and notification parameters.

Chapter 9, **Spanning Tree Configuration**, describes how to review and set Spanning Tree bridge parameters for the device, including bridge priority, hello time, maximum aging time and forward delay; and how to review and set Spanning Tree port parameters, including port priority and path costs. Configuring the SpanGuard and Loop Protect functions is also described.

Chapter 10, **802.1Q VLAN Configuration**, describes how to create static VLANs, select the mode of operation for each port, establish VLAN forwarding (egress) lists, route frames according to VLAN ID, display the current ports and port types associated with a VLAN and protocol, create a secure management VLAN, and configure ports on the device as GVRP-aware ports.

Chapter 11, **Policy Classification Configuration**, describes how to create, change or remove user roles or profiles based on business-specific use of network services; how to permit or deny access to specific services by creating and assigning classification rules which map user profiles to frame filtering policies; how to classify frames to a VLAN or Class of Service (CoS); and how to assign or unassign ports to policy profiles so that only ports activated for a profile will be allowed to transmit frames accordingly.

Chapter 12, **Port Priority Configuration**, describes how to set the transmit priority of each port and configure a rate limit for a given port and list of priorities.

Chapter 13, **IGMP Configuration**, describes how to configure Internet Group Management Protocol (IGMP) settings for multicast filtering.

Chapter 14, **Logging and Network Management**, describes how to configure Syslog, how to manage general switch settings, how to monitor network events and status,and how to configure SNTP and node aliases.

Chapter 15, **RMON Configuration**, describes how to use RMON (Remote Network Monitoring), which provides comprehensive network fault diagnosis, planning, and performance tuning information and allows for interoperability between SNMP management stations and monitoring agents.

Chapter 16, **DHCP Server Configuration**, describes how to review and configure DHCP server parameters, how to review and configure DHCP address pools, and how to display DHCP server information.

Chapter 17, **DHCP Snooping and Dynamic ARP Inspection**, describes two security features: DHCP snooping, which monitors DHCP messages between a DHCP client and DHCP server to filter harmful DHCP messages and to build a database of authorized address bindings, and Dynamic ARP inspection, which uses the bindings database created by the DHCP snooping feature to reject invalid and malicious ARP packets.

Chapter 18, **Preparing for Router Mode**, provides information about router modes.

Chapter 19, **IP Configuration**, describes how to enable IP routing for router mode operation, how to configure IP interface settings, how to review and configure the routing ARP table, how to review and configure routing broadcasts, how to configure PIM, and how to configure IP routes.

Chapter 20, **IPv4 Routing Protocol Configuration**, describes how to configure IPv4 routing and routing protocols, including RIP, OSPF, DVMRP, IRDP, and VRRP.

Chapter 21, **IPv6 Management**, describes the commands used to configure IPv6 at the switch level.

Chapter 22, **IPv6 Configuration**, describes the commands used to configure IPv6 at the routing level.

Chapter 23, **IPv6 Proxy Routing**, describes how to enable IPv6 proxy routing and how to configure a mixed C2/C3 stack for IPv6 proxy routing.

Chapter 24, **DHCPv6 Configuration**, describes the commands used to configure the Dynamic Host Configuration Protocol for IPv6.

Chapter 25, **OSPFv3 Configuration**, describes the commands used to configure the Open Shortest Path First routing protocol for IPv6.

Chapter 26, **Authentication and Authorization Configuration**, describes how to configure 802.1X authentication using EAPOL, how to configure RADIUS server, Secure Shell server, MAC authentication, MAC locking, Port Web Authentication, and IP access control lists (ACLs).

Chapter 27, **TACACS+ Configuration**, provides information about the commands used to configure and monitor TACACS+ (Terminal Access Controller Access-Control System Plus).

Chapter 28, **sFlow Configuration**, provides information about the commands used to configure and monitor the sFlow system.

Appendix A, **Policy and Authentication Capacities**, lists the policy and authentication capacities of the SecureStack C3 as of the date this document was published.

Related Documents

The following Enterasys Networks documents may help you to set up, control, and manage the SecureStack device:

- *Enterasys Firmware Feature Guides*
- SecureStack C3 Installation Guide(s)
- *SecureStack Redundant Power System Installation Guide*

Documents listed above, can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following web site:

http://www.enterasys.com/support/manuals/

Conventions Used in This Guide

The following conventions are used in the text of this document:

Convention	Description
Bold font	Indicates mandatory keywords, parameters or keyboard keys.
italic font	Indicates complete document titles.
`Courier` font	Used for examples of information displayed on the screen.
`Courier` font in italics	Indicates a user-supplied value, either required or optional.
[ ]	Square brackets indicate an optional value.
{ }	Braces indicate required values. One or more values may be required.
|	A vertical bar indicates a choice in values.
[x | y | z]	Square brackets with a vertical bar indicate a choice of a value.
{x | y | z}	Braces with a vertical bar indicate a choice of a required value.
[x {y | z}]	A combination of square brackets with braces and vertical bars indicates a required choice of an optional value.

The following icons are used in this guide:

Note: Calls the reader's attention to any item of information that may be of special importance.

Router: Calls the reader's attention to router-specific commands and information.

Caution: Contains information essential to avoid damage to the equipment.

Getting Help

For additional support related to this switch or document, contact Enterasys Networks using one of the following methods:

World Wide Web	http://www.enterasys.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-978-684-1000 For the Enterasys Networks Support toll-free number in your country: http://www.enterasys.com/support/contact/
Internet mail	support@enterasys.com To expedite your message, type **[C-SERIES]** in the subject line.

To send comments or suggestions concerning this document to the Technical Publications Department:

techpubs@enterasys.com

Make sure to include the document Part Number in the email message.

Before calling Enterasys Networks, have the following information ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (for example, layout, cable type)
- Network load and frame size at the time of trouble (if known)
- The switch history (for example, have you returned the switch before, is this a recurring problem?)
- Any previous Return Material Authorization (RMA) numbers

1

Introduction

This chapter provides an overview of the SecureStack C3's unique features and functionality, an overview of the tasks that may be accomplished using the CLI interface, an overview of ways to manage the switch, factory default settings, and information about how to use the Command Line Interface to configure the switch.

SecureStack C3 CLI Overview

The Enterasys Networks SecureStack C3 CLI interface allows you to perform a variety of network management tasks, including the following:

- Use CLI commands to perform network management and switch configuration operations.
- Download a new firmware image.
- Assign IP address and subnet mask.
- Select a default gateway.
- Establish and manage Virtual Local Area Networks (VLANs).
- Establish and manage policy profiles and classifications.
- Establish and manage priority classification.
- Configure IPv4 routing and routing protocols.
- Configure IPv6 routing and routing protocols, including OSPFv3.
- Configure security protocols, including 802.1X and RADIUS, SSHv2, PWA, MAC locking, and MAC authentication.
- Configure access control lists (ACLs).

Switch Management Methods

The SecureStack C3 switch can be managed using the following methods:

- Locally using a VT type terminal connected to the console port.
- Remotely using a VT type terminal connected through a modem.

- Remotely using an SNMP management station.
- In-band through a Telnet connection.
- In-band using the Enterasys NetSight® management application.
- Remotely using WebView™, Enterasys Networks' embedded web server application.

The *Installation Guide* for your SecureStack C3 device provides setup instructions for connecting a terminal or modem to the switch.

Factory Default Settings

The following tables list factory default settings available on the SecureStack C3 switch.

Table 1-1 Default Settings for Basic Switch Operation

Feature	Default Setting
Switch Mode Defaults	
CDP discovery protocol	Auto enabled on all ports.
CDP authentication code	Set to 00-00-00-00-00-00-00-00
CDP hold time	Set to 180 seconds.
CDP interval	Transmit frequency of CDP messages set to 60 seconds.
Cisco discovery protocol	Auto enabled on all ports.
Cisco DP hold time	Set to 180 seconds.
Cisco DP interval timer	Set to 60 seconds.
Community name	Public.
Console (serial) port required settings	Baud rate: 9600 Data bits: 8 Flow control: disabled Stop bits: 1 Parity: none
DHCP server	Disabled.
EAPOL	Disabled.
EAPOL authentication mode	When enabled, set to auto for all ports.
GARP timer	Join timer set to 20 centiseconds; leave timer set to 60 centiseconds; leaveall timer set to 1000 centiseconds.
GVRP	Globally enabled.
History buffer size	20 lines.
IEEE 802.1 authentication	Disabled.
IGMP snooping	Disabled. When enabled, query interval is set to 260 seconds and response time is set to 10 seconds.
IP mask and gateway	Subnet mask set to 0.0.0.0; default gateway set to 0.0.0.0.
IP routes	No static routes configured.
Jumbo frame support	Enabled on all ports.

Table 1-1 Default Settings for Basic Switch Operation (Continued)

Feature	Default Setting
Link aggregation control protocol (LACP)	Enabled.
Link aggregation admin key	Set to 32768 for all ports.
Link aggregation flow regeneration	Disabled.
Link aggregation system priority	Set to 32768 for all ports.
Link aggregation outport algorithm	Set to DIP-SIP.
Lockout	Set to disable Read-Write and Read-Only users, and to lockout the default admin (Super User) account for 15 minutes, after 3 failed login attempts.
Logging	Syslog port set to UDP port number 514. Logging severity level set to 6 (significant conditions) for all applications.
MAC aging time	Set to 300 seconds.
MAC locking	Disabled (globally and on all ports).
Passwords	Set to an empty string for all default user accounts. User must press ENTER at the password prompt to access CLI.
Password aging	Disabled.
Password history	No passwords are checked for duplication.
Policy classification	Classification rules are automatically enabled when created.
Port auto-negotiation	Enabled on all ports.
Port advertised ability	Maximum ability advertised on all ports.
Port broadcast suppression	Enabled and set to limit broadcast packets to 14,881 per second on all switch ports.
Port duplex mode	Set to half duplex, except for 100BASE-FX and 1000BASE-X, which is set to full duplex.
Port enable/disable	Enabled.
Port priority	Set to 0.
Port speed	Set to 10 Mbps, except for 1000BASE-X, which is set to 1000 Mbps, and 100BASE-FX, which is set to 100 Mbps.
Port trap	All ports are enabled to send link traps.
Power over Ethernet port admin state	Administrative state is on (auto).
Priority classification	Classification rules are automatically enabled when created.
RADIUS client	Disabled.
RADIUS last resort action	When the client is enabled, set to Challenge.
RADIUS retries	When the client is enabled, set to 3.
RADIUS timeout	When the client is enabled, set to 20 seconds.
Rate limiting	Disabled (globally and on all ports).

Table 1-1 Default Settings for Basic Switch Operation (Continued)

Feature	Default Setting
SNMP	Enabled.
SNTP	Disabled.
Spanning Tree	Globally enabled and enabled on all ports.
Spanning Tree edge port administrative status	Edge port administrative status begins with the value set to **false** initially after the device is powered up. If a Spanning Tree BDPU is not received on the port within a few seconds, the status setting changes to **true**.
Spanning Tree edge port delay	Enabled.
Spanning Tree forward delay	Set to 15 seconds.
Spanning Tree hello interval	Set to 2 seconds.
Spanning Tree ID (SID)	Set to 0.
Spanning Tree maximum aging time	Set to 20 seconds.
Spanning Tree port priority	All ports with bridge priority are set to 128 (medium priority).
Spanning Tree priority	Bridge priority is set to 32768.
Spanning Tree topology change trap suppression	Enabled.
Spanning Tree version	Set to mstp (Multiple Spanning Tree Protocol).
SSH	Disabled.
System baud rate	Set to 9600 baud.
System contact	Set to empty string.
System location	Set to empty string.
System name	Set to empty string.
Terminal	CLI display set to 80 columns and 24 rows.
Timeout	Set to 5 minutes.
User names	Login accounts set to **ro** for Read-Only access; **rw** for Read-Write access; and **admin** for Super User access.
VLAN dynamic egress	Disabled on all VLANs.
VLAN ID	All ports use a VLAN identifier of 1.
Host VLAN	Default host VLAN is 1.

Not all of the following routing features are available on all platforms. Check the Release Notes for your specific platforms for details.

Table 1-2 Default Settings for Router Operation

Output...	What it displays...
Access groups (IP security)	None configured.
Access lists (IP security)	None configured.

Table 1-2 Default Settings for Router Operation (Continued)

Output...	What it displays...
Area authentication (OSPF)	Disabled.
Area default cost (OSPF)	Set to 1.
Area NSSA (OSPF)	None configured.
Area range (OSPF)	None configured.
ARP table	No permanent entries configured.
ARP timeout	Set to 14,400 seconds.
Authentication key (RIP and OSPF)	None configured.
Authentication mode (RIP and OSPF)	None configured.
Dead interval (OSPF)	Set to 40 seconds.
Disable triggered updates (RIP)	Triggered updates allowed.
Distribute list (RIP)	No filters applied.
DVMRP	Disabled. Metric set to 1.
Hello interval (OSPF)	Set to 10 seconds for broadcast and point-to-point networks. Set to 30 seconds for non-broadcast and point-to-multipoint networks.
ICMP	Enabled for echo-reply and mask-reply modes.
IP-directed broadcasts	Disabled.
IP forward-protocol	Enabled with no port specified.
IP interfaces	Disabled with no IP addresses specified.
IRDP	Disabled on all interfaces. When enabled, maximum advertisement interval is set to 600 seconds, minimum advertisement interval is set to 450 seconds, holdtime is set to 1800 seconds, and address preference is set to 0.
MD5 authentication (OSPF)	Disabled with no password set.
MTU size	Set to 1500 bytes on all interfaces.
OSPF	Disabled.
OSPF cost	Set to 10 for all interfaces.
OSPF network	None configured.
OSPF priority	Set to 1.
Passive interfaces (RIP)	None configured.
Proxy ARP	Enabled on all interfaces.
Receive interfaces (RIP)	Enabled on all interfaces.
Retransmit delay (OSPF)	Set to 1 second.
Retransmit interval (OSPF)	Set to 5 seconds.
RIP receive version	Set to accept both version 1 and version 2.
RIP send version	Set to version 1.
RIP offset	No value applied.
SNMP	Enabled.

Table 1-2 Default Settings for Router Operation (Continued)

Output...	What it displays...
Split horizon	Enabled for RIP packets without poison reverse.
Stub area (OSPF)	None configured.
Telnet	Enabled.
Telnet port (IP)	Set to port number 23.
Timers (OSPF)	SPF delay set to 5 seconds. SPF holdtime set to 10 seconds.
Transmit delay (OSPF)	Set to 1 second.
VRRP	Disabled.

Using the Command Line Interface

Starting a CLI Session

Connecting Using the Console Port

Connect a terminal to the local console port as described in your SecureStack C3 *Installation Guide*. The startup screen, Figure 1-1, will display on the terminal. You can now start the Command Line Interface (CLI) by

- using a default user account, as described in "Using a Default User Account" on page 1-7, or
- using an administratively-assigned user account as described in "Using an Administratively Configured User Account" on page 1-7.

Figure 1-1 SecureStack C3 Startup Screen

```
Username:admin
Password:

Enterasys SecureStack C3
Command Line Interface

Enterasys Networks, Inc.
50 Minuteman Rd.
Andover, MA 01810-1008 U.S.A.

Phone: +1 978 684 1000
E-mail: support@enterasys.com
WWW: http://www.enterasys.com

(c) Copyright Enterasys Networks, Inc. 2008

Chassis Serial Number:      041800249041
Chassis Firmware Revision:  6.03.xx.xxxx


C3(su)->
```

Connecting Using Telnet

Once the SecureStack C3 device has a valid IP address, you can establish a Telnet session from any TCP/IP based node on the network. For information about setting the switch's IP address, refer to "set ip address" on page 3-11.

To establish a Telnet session:

1. Telnet to the switch's IP address.
2. Enter login (user name) and password information in one of the following ways:
   - If the switch's default login and password settings have not been changed, follow the steps listed in "Using a Default User Account" on page 1-7, or
   - Enter an administratively-configured user name and password.

The notice of authorization and the prompt displays as shown in Figure 1-1.

For information about configuring Telnet settings, refer to "Starting and Configuring Telnet" on page 3-37.

Refer to the instructions included with the Telnet application for information about establishing a Telnet session.

Logging In

By default, the SecureStack C3 switch is configured with three user login accounts—**ro** for Read-Only access, **rw** for Read-Write access, and **admin** for super-user access to all modifiable parameters. The default password is set to a blank string. For information on changing these default settings, refer to "Setting User Accounts and Passwords" on page 3-2.

Using a Default User Account

If this is the first time you are logging in to the SecureStack C3 switch, or if the default user accounts have not been administratively changed, proceed as follows:

1. At the login prompt, enter one of the following default user names:
   - **ro** for Read-Only access.
   - **rw** for Read-Write access.
   - **admin** for Super User access.
2. Press ENTER. The Password prompt displays.
3. Leave this string blank and press ENTER. The switch information and prompt displays as shown in Figure 1-1.

Using an Administratively Configured User Account

If the switch's default user account settings have been changed, proceed as follows:

1. At the login prompt, enter your administratively-assigned user name and press ENTER.
2. At the Password prompt, enter your password and press ENTER.

The notice of authorization and the prompt displays as shown in Figure 1-1.

Note: Users with Read-Write (rw) and Read-Only access can use the set password command (page 3-5) to change their own passwords. Administrators with Super User (su) access can use the set system login command (page 3-4) to create and change user accounts, and the set password command to change any local account password.

Navigating the Command Line Interface

Getting Help with CLI Syntax

The SecureStack C3 switch allows you to display usage and syntax information for individual commands by typing **help** or **?** after the command.

CLI Command Defaults Descriptions

Each command description in this guide includes a section entitled "Defaults" which contains different information from the factory default settings on the switch described in Table 1-1. The section defines CLI behavior if the user enters a command without typing optional parameters (indicated by square brackets [ ]). For commands without optional parameters, the defaults section lists "None". For commands with optional parameters, this section describes how the CLI responds if the user opts to enter only the keywords of the command syntax. Figure 1-2 provides an example.

Figure 1-2 Sample CLI Defaults Description

Syntax

`show port status` [*`port-string`*]

Defaults

If *port-string* is not specified, status information for all ports will be displayed.

CLI Command Modes

Each command description in this guide includes a section entitled "Mode" which states whether the command is executable in Admin (Super User), Read-Write, or Read-Only mode. Users with Read-Only access will only be permitted to view Read-Only (**show**) commands. Users with Read-Write access will be able to modify all modifiable parameters in **set** and **show** commands, as well as view Read-Only commands. Administrators or Super Users will be allowed all Read-Write and Read-Only privileges, and will be able to modify local user accounts. The SecureStack C3 switch indicates which mode a user is logged in as by displaying one of the following prompts:

- Admin: C3(su)->
- Read-Write: C3(rw)->
- Read-Only: C3(ro)->

Performing Keyword Lookups

Entering a space and a question mark (**?**) after a keyword will display all commands beginning with the keyword. Figure 1-3 shows how to perform a keyword lookup for the **show snmp** command. In this case, four additional keywords are used by the **show snmp** command. Entering a space and a question mark (**?**) after any of these parameters (such as **show snmp community**) will display additional parameters nested within the syntax.

Figure 1-3 Performing a Keyword Lookup

```
C3(su)->show snmp ?

community               SNMP v1/v2c community name configuration
notify                  SNMP notify configuration
targetaddr              SNMP target address configuration
targetparams            SNMP target parameters configuration
```

Entering a question mark (**?**) without a space after a partial keyword will display a list of commands that begin with the partial keyword. Figure 1-4 shows how to use this function for all commands beginning with **co:**

Figure 1-4 Performing a Partial Keyword Lookup

```
C3(rw)->co?
configure                copy
C3(su)->co
```

Note: At the end of the lookup display, the system will repeat the command you entered without the ?.

Displaying Scrolling Screens

If the CLI screen length has been set using the **set length** command as described on page 3-29, CLI output requiring more than one screen will display `--More--` to indicate continuing screens. To display additional screen output:

- Press any key other than ENTER to advance the output one screen at a time.
- Press ENTER to advance the output one line at a time.

The example in Figure 1-5 shows how the **show mac** command indicates that output continues on more than one screen.

Figure 1-5 Scrolling Screen Output

```
C3(su)->show mac

MAC Address           FID       Port      Type
 ------------------------------------------------------------
 00-00-1d-67-68-69      1       host      Management
 00-00-02-00-00-00      1       ge.1.2    Learned
 00-00-02-00-00-01      1       ge.1.3    Learned
 00-00-02-00-00-02      1       ge.1.4    Learned
 00-00-02-00-00-03      1       ge.1.5    Learned
 00-00-02-00-00-04      1       ge.1.6    Learned
 00-00-02-00-00-05      1       ge.1.7    Learned
 00-00-02-00-00-06      1       ge.1.8    Learned
 00-00-02-00-00-07      1       ge.1.9    Learned
 00-00-02-00-00-08      1       ge.1.10   Learned
--More--
```

Abbreviating and Completing Commands

The SecureStack C3 switch allows you to abbreviate CLI commands and keywords down to the number of characters that will allow for a unique abbreviation. Figure 1-6 shows how to abbreviate the **show netstat** command to **sh net**.

Figure 1-6 Abbreviating a Command

```
C3(su)->sh net
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        State
----- ------ ------  --------------------- ---------------------- -------
TCP        0      0  10.21.73.13.23        134.141.190.94.51246   ESTABLISHED
TCP        0    275  10.21.73.13.23        134.141.192.119.4724   ESTABLISHED
TCP        0      0  *.80                  *.*                    LISTEN
TCP        0      0  *.23                  *.*                    LISTEN
UDP        0      0  10.21.73.13.1030      134.141.89.113.514
UDP        0      0  *.161                 *.*
UDP        0      0  *.1025                *.*
UDP        0      0  *.123                 *.*
```

Basic Line Editing Commands

The CLI supports EMACs-like line editing commands. Table 1-3 lists some commonly used commands.

Table 1-3 Basic Line Editing Commands

Key Sequence	Command
Ctrl+A	Move cursor to beginning of line.
Ctrl+B	Move cursor back one character.
Ctrl+D	Delete a character.
Ctrl+E	Move cursor to end of line.
Ctrl+F	Move cursor forward one character.
Ctrl+H	Delete character to left of cursor.
Ctrl+I or TAB	Complete word.
Ctrl+K	Delete all characters after cursor.
Ctrl+N	Scroll to next command in command history (use the CLI history command to display the history).
Ctrl+P	Scroll to previous command in command history.
Ctr1+Q	Resume the CLI process.
Ctr1+S	Pause the CLI process (for scrolling).
Ctrl+T	Transpose characters.
Ctrl+U or Ctrl+X	Delete all characters before cursor.
Ctrl+W	Delete word to the left of cursor.
Ctrl+Y	Restore the most recently deleted item.

2

Configuring Switches in a Stack

This chapter provides information about configuring SecureStack C3 switches in a stack.

About SecureStack C3 Switch Operation in a Stack

The SecureStack C3 products are stackable switches that can be adapted and scaled to help meet your network needs. These switches provide a management platform and uplink to a network backbone for a stacked group of up to eight SecureStack C3 switches.

Note: You can mix SecureStack C2 and C3 switches in a single stack, although only the lowest common denominator of functionality will be supported in a mixed stack. Refer to "Issues Related to Mixed Type Stacks" on page 2-5 for information about configuring a mixed stack.

Once installed in a stack, the switches behave and perform as a single switch product. As such, you can start with a single unit and add more units as your network expands. You can also mix different products in the family in a single stack to provide a desired combination of port types and functions to match the requirements of individual applications. In all cases, a stack of units performs as one large product, and is managed as a single network entity.

When switches are installed and connected as described in the SecureStack C3 Installation Guides, the following occurs during initialization:

- The switch that will manage the stack is automatically established. This is known as the manager switch.
- All other switches are established as members in the stack.
- The hierarchy of the switches that will assume the function of backup manager is also determined in case the current manager malfunctions, is powered down, or is disconnected from the stack.

- The console port on the manager switch remains active for out-of-band (local) switch management, but the console port on each member switch is deactivated. This enables you to set the IP address and system password using a single console port. Now each switch can be configured locally using only the manager's console port, or inband using a remote device and the CLI set of commands described in this section.

Once a stack is created (more than one switch is interconnected), the following procedure occurs:

1. By default, unit IDs are arbitrarily assigned on a first-come, first-served basis.
2. Unit IDs are saved against each module. Then, every time a board is power-cycled, it will initialize with the same unit ID. This is important for port-specific information (for example: ge.4.12 is the 12th Gigabit Ethernet port on Unit # 4).
3. The management election process uses the following precedence to assign a management switch:
   a. Previously assigned / elected management unit
   b. Management assigned priority (values 1-15)
   c. Hardware preference level
   d. Highest MAC Address

Use the following recommended procedures when installing a new stackable system or adding a new unit to an existing stack.

Important

The following procedures assume that all units have a clean configuration from manufacturing. When adding a new unit to an already running stack, it is also assumed that the new unit is using the same firmware image version as other units in the stack.

Installing a New Stackable System of Up to Eight Units

Use the following procedure for installing a new stack of up to eight units out of the box.

1. Before applying power, make **all** physical connections with the stack cables as described in the SecureStack C3 Installation Guides.
2. Once all of the stack cables have been connected, individually power on each unit from top to bottom.

Notes: Ensure that each switch is fully operational before applying power to the next switch. Since unit IDs are assigned on a first-come, first-served basis, this will ensure that unit IDs are ordered sequentially.

Once unit IDs are assigned, they are persistent and will be retained during a power cycle to any or all of the units.

3. (Optional) If desired, change the management unit using the **set switch movemanagement** command as described in "set switch movemanagement" on page 2-11.
4. Once the desired master unit has been selected, reset the system using the **reset** command (page 3-50).
5. After the stack has been configured, you can use the **show switch** *unit* command (page 2-6) to physically identify each unit. When you enter the command with a unit number, the MGR LED of the specified switch will blink for 10 seconds. The normal state of this LED is off for member units and steady green for the manager unit.

Installing Previously-Configured Systems in a Stack

If member units in a stack have been previous members of a different stack, you may need to configure the renumbering of the stack as follows:

1. Stack the units in the method desired, and connect the stack cables.
2. Power up only the unit you wish to be manager.
3. Once the management unit is powered up, log into the CLI, and use the **show switch** command as described in "show switch" on page 2-6 to display stacking information.
4. Clear any switches which are listed as "unassigned" using the **clear switch member** command as described in "clear switch member" on page 2-12.
5. Power up the member of the stack you wish to become unit 2. Once the second unit is fully powered, the COM session of the CLI will state that a new CPU was added.
6. Use the **show switch** command to redisplay stacking information.
   a. If the new member displays as unit 2, you can proceed to repeat this step with the next unit.
   b. If the new member displays a different unit number, you must:
      (1) Renumber the stack using the **set switch renumber** command as described in "set switch" on page 2-9, then
      (2) Clear the original unit number using the **clear switch member** command.
7. Repeat Step 6 until all members have been renumbered in the order you desire.
8. After the stack has been reconfigured, you can use the **show switch** *unit* command ("show switch" on page 2-6) to physically confirm the identity of each unit. When you enter the command with a unit number, the MGR LED of the specified switch will blink for 10 seconds. The normal state of this LED is off for member units and steady green for the manager unit.

Adding a New Unit to an Existing Stack

Use the following procedure for installing a new unit to an existing stack configuration. This procedure assumes that the new unit being added has a clean configuration from manufacturing and is running the same firmware image version as other units in the stack.

1. Ensure that power is off on the new unit being installed.
2. Use one of the following methods to complete stack cable connections:
   – If the running stack uses a daisy chain topology, make the stack cable connections from the bottom of the stack to the new unit (that is, STACK DOWN port from the bottom unit of the running stack to the STACK UP port on the new unit).
   – If the running stack uses a ring stack topology, break the ring and make the stack cable connections to the new unit to close the ring.
3. Apply power to the new unit.

Creating a Virtual Switch Configuration

You can create a configuration for a SecureStack C3 switch before adding the actual physical device to a stack. This preconfiguration feature includes configuring protocols on the ports of the "virtual switch."

To create a virtual switch configuration in a stack environment:

1. Display the types of switches supported in the stack, using the **show switch switchtype** command (page 2-7).
2. Using the output of the **show switch switchtype** command, determine the switch index (SID) of the model of switch being configured.
3. Add the virtual switch to the stack using the **set switch member** command (page 2-11). Use the SID of the switch model, determined in the previous step, and the unit ID that you want to assign to this switch member.
4. Proceed to configure the ports of the virtual switch as you would do for physically present devices.

The following example adds a C3G124-24 mode to a stack as unit 2 of the stack. The first port on that virtual switch is then associated with VLAN 555.

```
C3(su)->show switch switchtype
                                        Mgmt   Code
SID         Switch Model ID             Pref  Version
--- ------------------------------- ---- ---------
1   C2G124-24                       1    0xa08245
2   C2K122-24                       1    0xa08245
3   C2G124-48                       1    0xa08245
4   C2G124-48P                      1    0xa08245
5   C2H124-48                       1    0xa08245
6   C2H124-48P                      1    0xa08245
7   C2G134-24P                      1    0xa08245
8   C2G170-24                       1    0xa08245
9   C3G124-24P                      1    0xa08245
10  C3G124-48P                      1    0xa08245
11  C3G124-48                       1    0xa08245
12  C3G124-24                       1    0xa08245
13  C3K172-24                       1    0xa08245
15  C3K122-24                       1    0xa08245
17  C3K122-24P                      1    0xa08245

C3(su)->set switch member 2 12
C3(su)->show switch
       Management    Preconfig     Plugged-in         Switch          Code
Switch    Status      Model ID      Model ID           Status         Version
------ ------------ ------------ ------------ -------------------- --------
1      Mgmt Switch  C3G124-48     C3G124-48     OK                  6.03.xx.xxxx
2      Unassigned   C3G124-24                    Not Present          00.00.00

C3(su)->set vlan create 555
C3(su)->clear vlan egress 1 ge.2.1
C3(su)->set port vlan ge.2.1 555 untagged
C3(su)->show port vlan ge.2.1
ge.2.1 is set to 555
```

Note: If you preconfigure a virtual switch and then add a physical switch of a different type to the stack as that unit number, any configured functionality that cannot be supported on the physical switch will cause a configuration mismatch status for that device and the ports of the new device will join detached. You must clear the mismatch before the new device will properly join the stack.

Considerations About Using Clear Config in a Stack

When using the **clear config** command (page 3-51) to clear configuration parameters in a stack, it is important to remember the following:

- Use **clear config** to clear config parameters without clearing stack unit IDs. This command WILL NOT clear stack parameters or the IP address and avoids the process of renumbering the stack.
- Use **clear config all** when it is necessary to clear all config parameters, including stack unit IDs and switch priority values. This command will not clear the IP address nor will it remove an applied advanced feature license.
- Use **clear ip address** to remove the IP address of the stack.
- Use **clear license** to remove an applied license from a switch.

Configuration parameters and stacking information can also be cleared **on the master unit only** by selecting the "restore configuration to factory defaults" option from the boot menu on switch startup. This selection will leave stacking priorities on all other units.

Issues Related to Mixed Type Stacks

Feature Support

Because the SecureStack C2 and C3 switches have different hardware architectures, the functionality supported by the two switch types is different. When the two types of switches are mixed in a stack, the functionality supported will be the lowest common denominator of features supported on all platforms. Refer to the firmware Release Notes for information about supported features.

Configuration

Common Firmware Version

Mixed stacking is supported by SecureStack C2 firmware version 5.02.xx.xxxx only. You can install the C2 firmware first, with the C3 switch in stand-alone mode, or you can add the C3 switch to the stack and then copy the C2 firmware to the C3 switch using the set switch copy-fw command (page 2-10). After copying the C2 firmware to the C3 switch, you must reset the stack.

Switch Manager

It is recommended that a SecureStack C3 switch be made the manager of a mixed stack. Use the set switch movemanagement command (page 2-11) to change the manager unit.

Stacking Configuration and Management Commands

Purpose

To review, individually configure and manage switches in a SecureStack C3 stack.

Commands

show switch

Use this command to display information about one or more units in the stack.

Syntax

`show switch [status]` [*`unit`*]

Parameters

status	(Optional) Displays power and administrative status information for one or more units in the stack.
unit	(Optional) Specifies the unit(s) for which information will display.

Defaults

If not specified, status and other configuration information about all units will be displayed.

Mode

Switch command, read-only.

Usage

After a stack has been configured, you can use this command to physically confirm the identity of each unit. When you enter the command with a unit number, the MGR LED of the specified switch will blink for 10 seconds. The normal state of this LED is off for member units and steady green for the manager unit.

Examples

This example shows how to display information about all switch units in the stack:

```
C3(rw)->show switch
        Management    Preconfig     Plugged-in         Switch          Code
Switch    Status      Model ID      Model ID           Status         Version
------ ------------ ------------- ------------- --------------------- --------
1      Mgmt Switch  C3G124-24     C3G124-24     OK                  06.03.xx.xxxx
2      Stack Member C3G124-24     C3G124-24     OK                  06.03.xx.xxxx
3      Stack Member C3G124-24     C3G124-24     OK                  06.03.xx.xxxx
4      Stack Member C3G124-24     C3G124-24     OK                  06.03.xx.xxxx
5      Stack Member C3G124-24     C3G124-24     OK                  06.03.xx.xxxx
6      Stack Member C3G124-24     C3G124-24     OK                  06.03.xx.xxxx
7      Stack Member C3G124-24     C3G124-24     OK                  06.03.xx.xxxx
8      Stack Member C3G124-24     C3G124-24     OK                  06.03.xx.xxxx
```

This example shows how to display information about switch unit 1 in the stack:

```
C3(ro)->show switch 1
Switch                              1
Management Status                   Management Switch
Hardware Management Preference      Unassigned
Admin Management Preference         Unassigned
Switch Type                         C3G124-24
Preconfigured Model Identifier      C3G124-24
Plugged-in Model Identifier         C3G124-24
Switch Status                       OK
Switch Description                  Enterasys Networks, Inc. C3 -- Model
                                    C3G124-24
Detected Code Version               06.03.xx.xxxx
Detected Code in Flash              03.01.20
Detected Code in Back Image         02.01.37
Up Time                             0 days 6 hrs 37 mins 54 secs
```

This example shows how to display status information for switch unit 1 in the stack:

```
C3(ro)->show switch status 1
Switch                              1
Switch Status                       Full
Admin State
Power State
Inserted Switch:
   Model Identifier                 C3G124-24
   Description                      Enterasys Networks, Inc. C3 -- Model
                                    C3G124-24
Configured Switch:
   Model Identifier                 C3G124-24
   Description                      Enterasys Networks, Inc. C3 -- Model
                                    C3G124-24
```

show switch switchtype

Use this command to display information about supported switch types in the stack.

Syntax

show switch switchtype [*switchindex*]

Parameters

switchindex	(Optional) Specifies the switch index (SID) of the switch type to display.

Defaults

None.

Mode

Switch command, read-only.

Examples

This example shows how to display switch type information about all switches in the stack:

```
C3(ro)->show switch switchtype
                                    Mgmt   Code
SID         Switch Model ID         Pref  Version
--- ------------------------------ ---- ---------
1   C2G124-24                      1    0xa08245
2   C2K122-24                      1    0xa08245
3   C2G124-48                      1    0xa08245
4   C2G124-48P                     1    0xa08245
5   C2H124-48                      1    0xa08245
6   C2H124-48P                     1    0xa08245
7   C2G134-24P                     1    0xa08245
8   C2G170-24                      1    0xa08245
9   C3G124-24P                     1    0xa08245
10  C3G124-48P                     1    0xa08245
11  C3G124-48                      1    0xa08245
12  C3G124-24                      1    0xa08245
13  C3K172-24                      1    0xa08245
15  C3K122-24                      1    0xa08245
17  C3K122-24P                     1    0xa08245
```

This example shows how to display switch type information about SID1:

```
C3(ro)->show switch switchtype 1
Switch Type                       0x56950200
Model Identifier                  C2G124-24
Switch Description                Enterasys Networks, Inc. C2 --
                                  Model  C2G124-24
Management Preference             1
Expected Code Version             0xa08245

Supported Cards:

   Slot                           0
   Card Index (CID)               1
   Model Identifier               C2G124-24
```

show switch stack-ports

Use this command to display various data flow and error counters on stack ports.

Syntax

show switch stack-ports [*unit*]

Parameters

unit	(Optional) Specifies the switch unit ID, an integer ranging from 1 to 8.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display data and error information on stack ports:

```
C3(ro)->show switch stack-ports
                   ------------TX-------------- ------------RX-----------
                   Data    Error                Data    Error
         Stacking  Rate    Rate      Total      Rate    Rate      Total
Switch     Port    (Mb/s) (Errors/s)  Errors    (Mb/s) (Errors/s)  Errors
------ ---------- ------ ---------- ---------- ------ ---------- --------
1      Up         0      0          0          0      0          0
       Down       0      0          0          0      0          0
```

set switch

Use this command to assign a switch ID, to set a switch's priority for becoming the management switch if the previous management switch fails, or to change the switch unit ID for a switch in the stack.

Syntax

set switch {*unit* [**priority** *value* | **renumber** *newunit*]}

Parameters

unit	Specifies a unit number for the switch. Value can range from 1 to 8.
priority *value*	Specifies a priority value for the unit. Valid values are 1 to 15 with higher values assigning higher priority.
renumber *newunit*	Specifies a new number for the unit.  **Note:** This number must be a previously unassigned unit ID number.

Defaults

None.

Mode

Switch command, read-write.

Examples

This example shows how to assign priority 3 to switch 5:

```
C3(su)->set switch 5 priority 3
```

This example shows how to renumber switch 5 to switch 7:

```
C3(su)->set switch 5 renumber 7
```

set switch copy-fw

Use this command to replicate the code image file from the management switch to other switch(es) in the stack.

Syntax

set switch copy-fw [**destination-system** *unit*]

Parameters

destination-system *unit*	(Optional) Specifies the unit number of unit on which to copy the management image file.

Defaults

If **destination-system** is not specified, the management image file will be replicated to all switches in the stack.

Mode

Switch command, read-write.

Example

This example shows how to replicate the management image file to all switches in the stack:

```
C3(su)->set switch copy-fw
 Are you sure you want to copy firmware? (y/n) y

 Code transfer completed successfully.
```

set switch description

Use this command to assign a name to a switch in the stack.

Syntax

set switch description *unit description*

Parameters

unit	Specifies a unit number for the switch.
description	Specifies a text description for the unit.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to assign the name “FirstUnit” to switch unit 1 in the stack:

```
C3(su)->set switch description 1 FirstUnit
```

set switch movemanagement

Use this command to move management switch functionality from one switch to another.

Syntax

set switch movemanagement *fromunit tounit*

Parameters

fromunit	Specifies the unit number of the current management switch.
tounit	Specifies the unit number of the newly-designated management switch.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to move management functionality from switch 1 to switch 2:

```
C3(su)->set switch movemenagement 1 2
Moving stack management will unconfigure entire stack including all interfaces.
Are you sure you want to move stack management? (y/n) y
```

set switch member

Use this command to add a virtual member to a stack. This allows you to preconfigure a switch before the physical device is actually added to the stack.

Syntax

set switch member *unit switch-id*

Parameters

unit	Specifies a unit number for the switch.
switch-id	Specifies a switch ID (SID) for the switch. SIDs can be displayed with the show switch switchtype command.

Defaults

None.

Mode

Switch command, read-write.

Usage

Refer to "Creating a Virtual Switch Configuration" on page 2-3 for more information about how to add a virtual switch to a stack.

Example

This example shows how to specify a switch as unit 1 with a switch ID of 1:

```
C3(su)->set switch member 1 1
```

clear switch member

Use this command to remove a member entry from the stack.

Syntax

clear switch member *unit*

Parameters

unit	Specifies the unit number of the switch.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to remove the switch 5 entry from the stack:

```
C3(su)->clear switch member 5
```

3

Basic Configuration

At startup, the SecureStack C3 switch is configured with many defaults and standard features. This chapter describes how to customize basic system settings to adapt to your work environment.

Quick Start Setup Commands

The tables in this section provide a quick reference for the CLI commands needed to begin basic C3 switch operation. Table 3-1 lists tasks and their associated CLI commands required for setting up the switch with the latest firmware. Table 3-2 lists optional CLI commands that will help you perform additional basic configuration on the switch. Refer to the pages listed for more information about each command.

Table 3-1 Required CLI Setup Commands

Step	Task	CLI commands	Refer to page...
1	Set a new password.	**set password** [*username*]	3-5
2	Set the switch IP address.	**set ip address** *ip-address* [**mask** *ip-mask*] [**gateway** *ip-gateway*]	3-11
3	Download, activate, and verify new firmware on the switch using TFTP copy.	**copy tftp://***tftp_server_ip_address/filename* **system:image**	3-45
		set boot system *filename*	3-36
		show version	3-26

Table 3-2 Optional CLI Setup Commands

Task	CLI commands	Refer to page...
Save the active configuration.	**save config**	3-41
Enable or disable SSH.	**set ssh enable** | **disable**	26-77
Enable or disable Telnet.	**set telnet** {**enable** | **disable**} [**inbound** | **outbound** | **all**]	3-37
Enable or disable HTTP management (WebView).	**set webview** {**enable** | **disable**}	3-53
Enable or disable SNMP port link traps.	**set port trap** *port-string* {**enable** | **disable**}	7-25
Set the per port broadcast limit	**set port broadcast** *port-string threshold-value*	7-34
Configure a VLAN.	**set vlan create** *vlan-id*	10-5
	set port vlan *port-string vlan-id* **modify-egress**	10-9
Set a Syslog server IP and severity	**set logging server** *index* **ip-addr** *ip-addr* **severity** *severity* **state enable**	10-9
Configure and enable a RADIUS server.	**set radius server** *index ip-addr port* [*secret-value*]{**realm** {**management-access** | **any** | **network-access**}	26-7
	set radius enable	26-7

Setting User Accounts and Passwords

Purpose

To change the switch's default user login and password settings, and to add new user accounts and passwords.

Commands

For information about...	Refer to page...
show system login	3-3
set system login	3-4
clear system login	3-4
set password	3-5
set system password length	3-6
set system password aging	3-6
set system password history	3-7
show system lockout	3-7
set system lockout	3-8

show system login

Use this command to display user login account information.

Syntax

show system login

Parameters

None.

Defaults

None.

Mode

Switch command, super user.

Example

This example shows how to display login account information. In this case, switch defaults have not been changed:

```
C3(su)->show system login
Password history size: 0
Password aging       : disabled

Username        Access      State

admin           super-user  enabled
ro              read-only   enabled
rw              read-write  enabled
```

Table 3-1 provides an explanation of the command output.

Table 3-1 show system login Output Details

Output Field	What It Displays...
Password history size	Number of previously used user login passwords that will be checked for duplication when the set password command is executed. Configured with set system password history (page 3-7).
Password aging	Number of days user passwords will remain valid before aging out. Configured with set system password aging (page 3-6).
Username	Login user names.
Access	Access assigned to this user account: super-user, read-write or read-only.
State	Whether this user account is enabled or disabled.

set system login

Use this command to create a new user login account, or to disable or enable an existing account. The SecureStack C3 switch supports up to 16 user accounts, including the **admin** account, which cannot be deleted.

Syntax

set system login *username* {**super-user** | **read-write** | **read-only**} {**enable** | **disable**}

Parameters

username	Specifies a login name for a new or existing user. This string can be a maximum of 80 characters, although a maximum of 16 characters is recommended for proper viewing in the **show system login** display.
super-user | **read-write** | **read-only**	Specifies the access privileges for this user.
enable | **disable**	Enables or disables the user account.

Defaults

None.

Mode

Switch command, super user.

Usage

Login accounts, including the **admin** user account, can be locked out after multiple failed attempts to log in to the system. Refer to "show system lockout" on page 3-7 and "set system lockout" on page 3-8 for more information about lockout parameters.

If the **admin** user account has been locked out, you must wait until the configured lockout time period has expired or you can power cycle the switch to reboot it, which will re-enable the **admin** user account.

Example

This example shows how to enable a new user account with the login name "netops" with super user access privileges:

```
C3(su)->set system login netops super-user enable
```

clear system login

Use this command to remove a local login user account.

Syntax

clear system login *username*

Parameters

username	Specifies the login name of the account to be cleared.  **Note:** The default admin (su) account cannot be deleted.

Defaults

None.

Mode

Switch command, super user.

Example

This example shows how to remove the “netops” user account:

```
C3(su)->clear system login netops
```

set password

Use this command to change system default passwords or to set a new login password on the CLI.

Syntax

set password [*username*]

Parameters

username	(Only available to users with super-user access.) Specifies a system default or a user-configured login account name. By default, the SecureStack C3 switch provides the following account names: **ro** for Read-Only access. **rw** for Read-Write access. **admin** for Super User access. (This access level allows Read-Write access to all modifiable parameters, including user accounts.)

Defaults

None.

Mode

Switch command, read-write.

Switch command, super-user.

Usage

Read-Write users can change their own passwords.

Super Users (Admin) can change any password on the system.

If you forget the password for the **admin** user account, you can reset the password to the default password value by pressing the password reset button on the switch.

Examples

This example shows how a super-user would change the Read-Write password from the system default (blank string):

```
C3(su)->set password rw
Please enter new password: ********
Please re-enter new password: ********
Password changed.
C3(su)->
```

This example shows how a user with Read-Write access would change his password:

```
C3(su)->set password
Please enter old password: ********
Please enter new password: ********
Please re-enter new password: ********
Password changed.
C3(su)->
```

set system password length

Use this command to set the minimum user login password length.

Syntax

set system password length *characters*

Parameters

characters	Specifies the minimum number of characters for a user account password. Valid values are 0 to 40.

Defaults

None.

Mode

Switch command, super user.

Example

This example shows how to set the minimum system password length to 8 characters:

```
C3(su)->set system password length 8
```

set system password aging

Use this command to set the number of days user passwords will remain valid before aging out, or to disable user account password aging.

Syntax

set system password aging {*days* | **disable**}

Parameters

days	Specifies the number of days user passwords will remain valid before aging out. Valid values are 1 to 365.
disable	Disables password aging.

Defaults

None.

Mode

Switch command, super user.

Example

This example shows how to set the system password age time to 45 days:

```
C3(su)->set system password aging 45
```

set system password history

Use this command to set the number of previously used user login passwords that will be checked for password duplication. This prevents duplicate passwords from being entered into the system with the **set password** command.

Syntax

set system password history *size*

Parameters

size	Specifies the number of passwords checked for duplication. Valid values are 0 to 10.

Defaults

None.

Mode

Switch command, super user.

Example

This example shows how to configure the system to check the last 10 passwords for duplication

```
C3(su)->set system password history 10
```

show system lockout

Use this command to display settings for locking out users after failed attempts to log in to the system.

Syntax

show system lockout

Parameters

None.

Defaults

None.

Mode

Switch command, super user.

Example

This example shows how to display user lockout settings. In this case, switch defaults have not been changed:

```
C3(su)->show system lockout
Lockout attempts: 3
Lockout time:     15 minutes.
```

Table 3-3 provides an explanation of the command output. These settings are configured with the **set system lockout** command ("set system lockout" on page 3-8).

Table 3-3 show system lockout Output Details

Output Field	What It Displays...
Lockout attempts	Number of failed login attempts allowed before a read-write or read-only user's account will be disabled.
Lockout time	Number of minutes the default admin user account will be locked out after the maximum login attempts.

set system lockout

Use this command to set the number of failed login attempts before locking out (disabling) a read-write or read-only user account, and the number of minutes to lockout the default admin super user account after maximum login attempts.

Syntax

set system lockout {[**attempts** *attempts*] [**time** *time*]}

Parameters

attempts *attempts*	Specifies the number of failed login attempts allowed before a read-write or read-only user's account will be disabled. Valid values are 1 to 10.
time *time*	Specifies the number of minutes the default admin user account will be locked out after the maximum login attempts. Valid values are 0 to 60.

Defaults

None.

Mode

Switch command, super user.

Usage

Once a user account is locked out, it can only be re-enabled by a super user with the **set system login** command (page 3-4).

If the default admin super user account has been locked out, you can wait until the lock out time has expired or you can reset the switch in order to re-enable the admin account.

Example

This example shows how to set login attempts to 5 and lockout time to 30 minutes:

```
C3(su)->set system lockout attempts 5 time 30
```

Setting Basic Switch Properties

Purpose

To display and set the system IP address and other basic system (switch) properties.

Commands

For information about...	Refer to page...
show ip address	3-10
set ip address	3-11
clear ip address	3-11
show ip protocol	3-12
set ip protocol	3-12
show system	3-13
show system hardware	3-14
show system utilization	3-15
set system utilization	3-16
clear system utilization	3-17
show system enhancedbuffermode	3-17
set system enhancedbuffermode	3-18
set system temperature	3-18
clear system temperature	3-19
show time	3-20
set time	3-20
show summertime	3-21
set summertime	3-22
set summertime date	3-22
set summertime recurring	3-23

show ip address

Use this command to display the system IP address and subnet mask.

Syntax

`show ip address`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the system IP address and subnet mask:

```
C3(su)->show ip address
Name                    Address                 Mask
----------------        ----------------        ----------------
host                    10.42.13.20             255.255.0.0
```

set ip address

Use this command to set the system IP address, subnet mask and default gateway.

Note: The C3 does not support the ability for a user to configure the host's gateway to be a local routed interface IP. The host's gateway must exist on a different device in the network if one is configured.

Syntax

set ip address *ip-address* [**mask** *ip-mask*] [**gateway** *ip-gateway*]

Parameters

ip-address	Sets the IP address for the system. For SecureStack C3 systems, this is the IP address of the management switch as described in "About SecureStack C3 Switch Operation in a Stack" on page 2-1.
mask *ip-mask*	(Optional) Sets the system's subnet mask.
gateway *ip-gateway*	(Optional) Sets the system's default gateway (next-hop device).

Defaults

If not specified, *ip-mask* will be set to the natural mask of the *ip-address* and *ip-gateway* will be set to the *ip-address*.

Mode

Switch command, read-write.

Usage

Parameters must be entered in the order shown (host IP, then mask, then gateway) for the command to be accepted.

Example

This example shows how to set the system IP address to 10.1.10.1 with a mask of 255.255.128.0:

```
C3(su)->set ip address 10.1.10.1 mask 255.255.128.0
```

clear ip address

Use this command to clear the system IP address.

Syntax

clear ip address

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the system IP address:

```
C3(rw)->clear ip address
```

show ip protocol

Use this command to display the method used to acquire a network IP address for switch management.

Syntax

show ip protocol

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the method used to acquire a network IP address:

```
C3(su)->show ip protocol
System IP address acquisition method: dhcp
```

set ip protocol

Use this command to specify the protocol used to acquire a network IP address for switch management.

Syntax

set ip protocol {bootp | dhcp | none}

Parameters

bootp	Selects BOOTP as the protocol to use to acquire the system IP address.
dhcp	Selects DHCP as the protocol to use to acquire the system IP address.
none	No protocol will be used to acquire the system IP address.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the method used to acquire a network IP address to DHCP.

```
C3(su)->set ip protocol dhcp
```

show system

Use this command to display system information, including contact information, power and fan tray status and uptime.

Syntax

show system

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display system information:

```
C3(su)->show system
System contact:
System location:
System name:

Switch 1
--------
PS1-Status                      PS2-Status
----------                      ----------
Ok                              Not Installed and/or Not Operating

Fan1-Status                     Fan2-Status
-----------                     -----------
Ok                              Ok

Temp-Alarm
-----------
off
Thermal Threshold: 58%
Temp alarm max threshold:  100%
Temp alarm trap: disabled
Temp alarm syslog: disabled

Uptime d,h:m:s  Logout
--------------  -------
0,20:36:49      0 min
```

The following table provides an explanation of the command output.

Table 3-4 show system Output Details

Output	What It Displays...
System contact	Contact person for the system. Default of a blank string can be changed with the **set system contact** command (“set system contact” on page 3-28).
System location	Where the system is located. Default of a blank string can be changed with the **set system location** command (“set system location” on page 3-28).
System name	Name identifying the system. Default of a blank string can be changed with the **set system name** command (“set system name” on page 3-27).
Switch x	Indicates the switch position in the stack. When multiple switches are in a stack, information for each switch is displayed.
PS1-Status	Operational status for the primary power supply.
PS2-Status	Operational status for the secondary power supply, if installed.
Fan*x*-Status	Operational status of the fan(s).
Temp-Alarm	Indicates status of temperature alarm — on, off. The status will show NA (not available) on switches that do not support this functionality.
Thermal Threshold	Percentage of thermal threshold reached. The status will show NA (not available) on switches that do not support this functionality.
Temp alarm max threshold	The temperature alarm threshold expressed as a percentage of the maximum rated. The default value is 100%.
Temp alarm trap	Indicates whether the sending of temperature alarm traps is enabled or disabled. The default is disabled.
Temp alarm syslog	Indicates whether temperature alarm syslog messages are enabled or disabled. The default is disabled.
Uptime d,h:m:s	System uptime.
Logout	Time an idle console or Telnet CLI session will remain connected before timing out. Default of 5 minutes can be changed with the **set logout** command (“set logout” on page 3-30).

show system hardware

Use this command to display the system’s hardware configuration.

Syntax

```
show system hardware
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the system's hardware configuration. Please note that the information you see displayed may differ from this example.

```
C3(su)->show system hardware
        SLOT 1 HARDWARE INFORMATION
        ---------------------------
        Model:
        Serial Number:                  777777777777
        Vendor ID:                      0xbc00
        Base MAC Address:               00:11:88:B1:76:C0
        Hardware Version:               BCM56514 REV 1
        FirmWare Version:               01.00.00.0052
        Boot Code Version:              01.00.42
```

show system utilization

Use this command to display detailed information about the processor running on the switch, or the overall memory usage of the Flash and SDRAM storage devices on the unit, or the processes running on the switch. Only the memory usage in the master unit of a stack is shown.

Syntax

show system utilization {**cpu** | **storage** | **process**}

Parameters

cpu	Display information about the processor running on the switch.
storage	Display information about the overall memory usage on the switch.
process	Display information about the processes running on the switch.

Defaults

None.

Mode

Switch command, read-only.

Examples

This example shows how to display the system's CPU utilization:

```
C3(ro)->show system utilization cpu

CPU Utilization Threshold Traps enable: Threshold = 80.0%

Total CPU Utilization:

Switch   CPU       5 sec      1 min       5 min
-----------------------------------------------
1        1         50%        49%         49%
```

This example shows how to display the system's overall memory usage:

```
C3(ro)->show system utilization storage
Storage Utilization:
Type    Description               Size(Kb)       Available (Kb)
-------------------------------------------------------------
RAM     RAM device                  262144                97173
Flash   Images, Config, Other       31095                 8094
```

This example shows how to display information about the processes running on the system. Only partial output is shown.

```
C3(ro)->show system utilization process
Switch:1    CPU:1

 TID     Name                        5Sec     1Min     5Min
-------------------------------------------------------------
 c157930 ipMapForwardingTask       3.60%    3.02%    3.48%
 cc70000 RMONTask                  0.00%    0.00%    0.00%
 ccb0b60 SNMPTask                 34.80%   34.06%   31.78%
 d4847a0 tEmWeb                    0.00%    0.03%    0.01%
 d4ca360 hapiRxTask                3.20%    4.80%    5.00%
 dec8600 lvl7TaskUtilMonitorTas    0.40%    0.40%    0.40%
 eb74120 bcmRX                     2.00%    2.91%    4.48%
 eb7fbc8 bcmLINK.0                 0.40%    0.22%    0.32%
 f00c9a0 bcmTX                     0.00%    0.33%    0.53%
 f027648 bcmCNTR.0                 0.00%    0.00%    0.03%
 f034858 bcmL2X.0                  0.00%    0.02%    0.04%
```

set system utilization

Use this command to set the threshold for sending CPU utilization notification messages.

Syntax

set system utilization threshold *threshold*

Parameters

threshold *threshold*	Specifies a threshold value in 1/10 of a percent. Valid range is 1 to 1000. A value of 0 disables utilization notification messages.

Defaults

The default threshold value is 80%.

Mode

Switch command, read-write.

Usage

This command sets the percentage of system CPU utilitization that will cause a trap notification to be sent. After the threshold has been exceeded, additional notifications will be sent once a minute until the utilization has dropped back below the threshold.

Example

This example sets the CPU utilization threshold to 75%.

```
C3(rw)->set system utilization threshold 750
```

clear system utilization

Use this command to reset the CPU utilization threshold to the default of 80%.

Syntax

clear system utilization

Parameters

None.

Defaults

The default threshold value is 80%.

Mode

Switch command, read-write.

Example

This example resets the CPU utilization threshold to the default.

```
C3(rw)->show system utilization cpu

CPU Utilization Threshold Traps enable: Threshold = 75.0%

Total CPU Utilization:

Switch    CPU         5 sec      1 min      5 min
-------------------------------------------------
1         1             10%        10%        10%

C3(rw)->clear system utilization
C3(rw)->show system utilization cpu

CPU Utilization Threshold Traps enable: Threshold = 80.0%

Total CPU Utilization:

Switch    CPU         5 sec      1 min      5 min
-------------------------------------------------
1         1             14%        11%        10%
```

show system enhancedbuffermode

Use this command to display the status of enhanced buffer mode, which optimizes buffer distribution into a single CoS queue operation for standalone switches or non-stacked switches.

Syntax

show system enhancedbuffermode

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to display enhanced buffer mode status:

```
C3(su)->show system enhancedbuffermode enable
Optimized system buffer distribution            Disable
```

set system enhancedbuffermode

Use this command to enable or disable enhanced buffer mode, which optimizes buffer distribution into a single CoS queue operation for standalone switches or non-stacked switches. Executing this command will reset the switch, so the system prompts you to confirm whether you want to proceed.

Syntax

set system enhancedbuffermode {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables enhanced buffer mode.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to enable enhanced buffer mode:

```
C3(su)->set system enhancedbuffermode enable

Changes in the enhanced buffer mode will require resetting this unit.
Are you sure you want to continue? (y/n)
```

set system temperature

Use this command to set the system high temperature threshold limit and the high temperature alert parameters, on the platforms that support this feature.

Syntax

set system temperature {[**syslog enable** | **disable**] [**trap enable** | **disable**] [**overtemp-threshold** *value*]}

Parameters

syslog enable | **disable**	Enables or disables logging high temperature alerts to the system log when the system transitions into an alarm state.
trap enable | **disable**	Enables or disables sending high temperature alerts by means of SNMP traps when the system transitions into an alarm state.
overtemp-threshold *value*	Sets the thermal threshold as a percentage of the maximum rated for the specific platform. Value can range from 0 to 100%.

Defaults

Syslog alerts are disabled by default.

Trap alerts are disabled by default.

Overtemp threshold is 100% by default.

Mode

Switch command, read-write.

Usage

On the platforms that support this feature, temperature sensors are located in several different locations within the device. Threshold calibrations have been calculated separately for each platform. The thermal overtemp threshold is the high-water mark that, when reached, triggers an alert to warn the system administrator that the device is operating at high temperatures.

When a high temperature alert condition occurs, the CPU LED on the front panel of the switch will flash red. In addition, if enabled, a syslog message will be logged and/or an SNMP trap will be sent.

The values set with this command can be viewed with the **show system** command.

Example

The following example enables sending SNMP traps and sets the overtemp threshold to 60%.

```
C3(su)->set system temperature trap enable overtemp-threshold 60
```

clear system temperature

Use this command to reset system high temperature parameters to their default values, on the platforms that support this feature.

Syntax

```
clear system temperature
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command resets all the high temperature parameters to their default values:

- Syslog alerts are disabled by default.
- Trap alerts are disabled by default.
- Overtemp threshold is 100% by default.

Example

This example resets all high temperature parameters to their defaults.

```
C3(su)->clear system temperature
```

show time

Use this command to display the current time of day in the system clock.

Syntax

show time

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the current time. The output shows the day of the week, month, day, and the time of day in hours, minutes, and seconds and the year:

```
C3(su)->show time
THU SEP 05 09:21:57 2002
```

set time

Use this command to change the time of day on the system clock.

Syntax

set time [*mm/dd/yyyy*] [*hh:mm:ss*]

Parameters

[*mm/dd/yyyy*] [*hh:mm:ss*]	Sets the time in: month, day, year and/or 24-hour format At least one set of time parameters must be entered.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the system clock to 7:50 a.m:

```
C3(su)->set time 7:50:00
```

show summertime

Use this command to display daylight savings time settings.

Syntax

show summertime

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display daylight savings time settings:

```
C3(su)->show summertime
Summertime is disabled and set to ''
Start : SUN APR 04 02:00:00 2004
End   : SUN OCT 31 02:00:00 2004
Offset: 60 minutes (1 hours 0 minutes)
Recurring: yes, starting at 2:00 of the first Sunday of April and ending at 2:00
 of the last Sunday of October
```

set summertime

Use this command to enable or disable the daylight savings time function.

Syntax

set summertime {**enable** | **disable**} [*zone*]

Parameters

enable | **disable**	Enables or disables the daylight savings time function.
zone	(Optional) Applies a name to the daylight savings time settings.

Defaults

If a *zone* name is not specified, none will be applied.

Mode

Switch command, read-only.

Example

This example shows how to enable daylight savings time function:

```
C3(su)->set summertime enable
```

set summertime date

Use this command to configure specific dates to start and stop daylight savings time. These settings will be non-recurring and will have to be reset annually.

Syntax

set summertime date *start_month start_date start_year start_hr_min end_month end_date end_year end_hr_min* [*offset_minutes*]

Parameters

start_month	Specifies the month of the year to start daylight savings time.
start_date	Specifies the day of the month to start daylight savings time.
start_year	Specifies the year to start daylight savings time.
start_hr_min	Specifies the time of day to start daylight savings time. Format is hh:mm.
end_month	Specifies the month of the year to end daylight savings time.
end_date	Specifies the day of the month to end daylight savings time.
end_year	Specifies the year to end daylight savings time.
end_hr_min	Specifies the time of day to end daylight savings time. Format is hh:mm.
offset_minutes	(Optional) Specifies the amount of time in minutes to offset daylight savings time from the non-daylight savings time system setting. Valid values are 1 - 1440.

Defaults

If an *offset* is not specified, none will be applied.

Mode

Switch command, read-write.

Example

This example shows how to set a daylight savings time start date of April 4, 2004 at 2 a.m. and an ending date of October 31, 2004 at 2 a.m. with an offset time of one hour:

```
C3(su)->set summertime date April 4 2004 02:00 October 31 2004 02:00 60
```

set summertime recurring

Use this command to configure recurring daylight savings time settings. These settings will start and stop daylight savings time at the specified day of the month and hour each year and will not have to be reset annually.

Syntax

set summertime recurring *start_week start_day start_month start_hr_min end_week end_day end_month end_hr_min* [*offset_minutes*]

Parameters

start_week	Specifies the week of the month to restart daylight savings time. Valid values are: first, second, third, fourth, and last.
start_day	Specifies the day of the week to restart daylight savings time.
start_hr_min	Specifies the time of day to restart daylight savings time. Format is hh:mm.
end_week	Specifies the week of the month to end daylight savings time.
end_day	Specifies the day of the week to end daylight savings time.
end_hr_min	Specifies the time of day to end daylight savings time. Format is hh:mm.
offset_minutes	(Optional) Specifies the amount of time in minutes to offset daylight savings time from the non-daylight savings time system setting. Valid values are 1 - 1440.

Defaults

If an *offset* is not specified, none will be applied.

Mode

Switch command, read-write.

Example

This example shows how set daylight savings time to recur starting on the first Sunday of April at 2 a.m. and ending the last Sunday of October at 2 a.m. with an offset time of one hour:

```
C3(su)->set summertime recurring first Sunday April 02:00 last Sunday October
02:00 60
```

clear summertime

Use this command to clear the daylight savings time configuration.

Syntax

clear summertime

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the daylight savings time configuration:

```
C3(su)->clear summertime
```

set prompt

Use this command to modify the command prompt.

Syntax

set prompt *prompt_string*

Parameters

prompt_string	Specifies a text string for the command prompt.

Note: A prompt string containing a space in the text must be enclosed in quotes as shown in the example below.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the command prompt to Switch 1:

```
C3(su)->set prompt “Switch 1”
Switch 1(su)->
```

show banner motd

Use this command to show the banner message of the day that will display at session login.

Syntax

`show banner motd`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the banner message of the day:

```
C3(rw)->show banner motd
        This system belongs to XYZ Corporation.
Use of this system is strictly limited to authorized personnel.
```

set banner motd

Use this command to set the banner message of the day displayed at session login.

Note: Banner message text must be enclosed in beginning and ending double quotation marks. The message itself cannot contain any additional double quotation marks.

Syntax

`set banner motd` *`message`*

Parameters

message	Specifies a message of the day. This is a text string that needs to be in double quotes if any spaces are used. Use a \n for a new line and \t for a tab (eight spaces).

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the message of the day banner to read: “This system belongs to XYZ Corporation. Use of this system is strictly limited to authorized personnel.”

```
C3(rw)->set banner motd "\tThis system belongs to XYZ Corporation.\nUse of this
system is strictly limited to authorized personnel."
```

clear banner motd

Use this command to clear the banner message of the day displayed at session login to a blank string.

Syntax

clear banner motd

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the message of the day banner to a blank string:

```
C3(rw)->clear banner motd
```

show version

Use this command to display hardware and firmware information. Refer to “Downloading a Firmware Image” on page 3-32 for instructions on how to download a firmware image.

Syntax

show version

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display version information. Please note that you may see different information displayed, depending on the type of hardware.

```
C3(su)->show version
Copyright (c) 2007 by Enterasys Networks, Inc.
```

```
 Model             Serial #            Versions
-------------  -----------------  -------------------
C3G124-48P       001188021035      Hw:BCM5665 REV 17
                                   Bp:01.00.29
                                   Fw:6.03.xx.xxxx
                                   BuFw:03.01.13
                                   PoE:500_3
```

Table 3-5 provides an explanation of the command output.

Table 3-5 show version Output Details

Output Field	What It Displays...
Model	Switch's model number.
Serial #	Serial number of the switch.
Versions	• Hw: Hardware version number. • Bp: BootPROM version. • Fw: Current firmware version number. • BuFw: Backup firmware version number. • PoE: Power over Ethernet driver version. (Displays only for PoE switches.)

set system name

Use this command to configure a name for the system.

Syntax

set system name [*string*]

Parameters

string	(Optional) Specifies a text string that identifies the system. **Note:** A name string containing a space in the text must be enclosed in quotes as shown in the example below.

Defaults

If *string* is not specified, the system name will be cleared.

Mode

Switch command, read-write.

Example

This example shows how to set the system name to Information Systems:

```
C3(su)->set system name “Information Systems”
```

set system location

Use this command to identify the location of the system.

Syntax

set system location [*string*]

Parameters

string	(Optional) Specifies a text string that indicates where the system is located. **Note:** A location string containing a space in the text must be enclosed in quotes as shown in the example below.

Defaults

If *string* is not specified, the location name will be cleared.

Mode

Switch command, read-write.

Example

This example shows how to set the system location string:

```
C3(su)->set system location “Bldg N32-04 Closet 9”
```

set system contact

Use this command to identify a contact person for the system.

Syntax

set system contact [*string*]

Parameters

string	(Optional) Specifies a text string that contains the name of the person to contact for system administration. **Note:** A contact string containing a space in the text must be enclosed in quotes as shown in the example below.

Defaults

If *string* is not specified, the contact name will be cleared.

Mode

Switch command, read-write.

Example

This example shows how to set the system contact string:

```
C3(su)->set system contact “Joe Smith”
```

set width

Use this command to set the number of columns for the terminal connected to the switch’s console port.

Syntax

set width *screenwidth [default]*

Parameters

screenwidth	Sets the number of terminal columns. Valid values are 50 to 150.
default	(Optional) Makes this setting persistent for all future sessions (written to NV-RAM).

Defaults

None.

Mode

Switch command, read-write.

Usage

The number of rows of CLI output displayed is set using the **set length** command as described in “set length” on page 3-29.

Example

This example shows how to set the terminal columns to 50:

```
C3(su)->set width 50
```

set length

Use this command to set the number of lines the CLI will display. This command is persistent (written to NV-RAM).

Syntax

set length *screenlength*

Parameters

screenlength	Sets the number of lines in the CLI display. Valid values are 0, which disables the scrolling screen feature described in “Displaying Scrolling Screens” on page 1-9, and from 5 to 512.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the terminal length to 50:

```
C3(su)->set length 50
```

show logout

Use this command to display the time (in seconds) an idle console or Telnet CLI session will remain connected before timing out.

Syntax

show logout

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the CLI logout setting:

```
C3(su)->show logout
Logout currently set to: 10 minutes.
```

set logout

Use this command to set the time (in minutes) an idle console or Telnet CLI session will remain connected before timing out.

Syntax

set logout *timeout*

Parameters

timeout	Sets the number of minutes the system will remain idle before timing out.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the system timeout to 10 minutes:

```
C3(su)->set logout 10
```

show console

Use this command to display console settings.

Syntax

show console [baud] [bits] [flowcontrol] [parity] [stopbits]

Parameters

baud	(Optional) Displays the input/output baud rate.
bits	(Optional) Displays the number of bits per character.
flowcontrol	(Optional) Displays the type of flow control.
parity	(Optional) Displays the type of parity.
stopbits	(Optional) Displays the number of stop bits.

Defaults

If no parameters are specified, all settings will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display all console settings:

```
C3(su)->show console
Baud    Flow     Bits  StopBits    Parity
------  -------  ----  ----------  ------
9600    Disable  8     1           none
```

set console baud

Use this command to set the console port baud rate.

Syntax

set console baud *rate*

Parameters

rate	Sets the console baud rate. Valid values are: 300, 600, 1200, 2400, 4800, 5760, 9600, 14400, 19200, 38400, and 115200.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the console port baud rate to 19200:

```
C3(su)->set console baud 19200
```

Downloading a Firmware Image

You can upgrade the operational firmware in the SecureStack C3 switch without physically opening the switch or being in the same location. There are two ways to download firmware to the switch:

- Via TFTP download. This procedure uses a TFTP server connected to the network and downloads the firmware using the TFTP protocol. For details on how to perform a TFTP download using the **copy** command, refer to "copy" on page 3-45. For information on setting TFTP timeout and retry parameters, refer to "set tftp timeout" on page 3-47 and "set tftp retry" on page 3-48.
- Via the serial (console) port. This procedure is an out-of-band operation that copies the firmware through the serial port to the switch. It should be used in cases when you cannot connect the switch to perform the in-band **copy** download procedure via TFTP. Serial console download has been successfully tested with the following applications:
  - HyperTerminal Copyright 1999
  - Tera Term Pro Version 2.3

Any other terminal applications may work but are not explicitly supported.

The C3 switch allows you to download and store dual images. The backup image can be downloaded and selected as the startup image by using the commands described in this section.

Downloading from a TFTP Server

To perform a TFTP download, proceed as follows:

1. If you have not already done so, set the switch's IP address using the **set ip address** command as detailed in "set ip address" on page 3-11.
2. Download a new image file using the **copy** command as detailed in "copy" on page 3-45.

Downloading via the Serial Port

To download switch firmware via the serial (console) port, proceed as follows:

1. With the console port connected, power up the switch. The following message displays:

```
Version 01.00.29 05-09-2005

Computing MD5 Checksum of operational code...
Select an option. If no selection in 2 seconds then
operational code will start.
```

```
1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2

Password: *************
```

2. Before the boot up completes, type **2 to select "Start Boot Menu". Use "administrator" for the Password**.

Note: The "Boot Menu" password "administrator" can be changed using boot menu option 11.

```
Boot Menu Version 01.00.29 05-09-2005


Options available
1  - Start operational code
2  - Change baud rate
3  - Retrieve event log using XMODEM (64KB).
4  - Load new operational code using XMODEM
5  - Display operational code vital product data
6  - Run Flash Diagnostics
7  - Update Boot Code
8  - Delete operational code
9  - Reset the system
10 - Restore Configuration to factory defaults (delete config files)
11 - Set new Boot Code password
[Boot Menu] 2
```

3. Type **2**. The following baud rate selection screen displays:

```
1 - 1200
2 - 2400
3 - 4800
4 - 9600
5 - 19200
6 - 38400
7 - 57600
8 - 115200
0 - no change
```

4. Type **8** to set the switch baud rate to 115200. The following message displays:

```
Setting baud rate to 115200, you must change your terminal baud rate.
```

5. Set the terminal baud rate to **115200** and press ENTER.

6. From the boot menu options screen, type **4** to load new operational code using XMODEM. When the XMODEM transfer is complete, the following message and header information will display:

```
[Boot Menu] 4
Ready to receive the file with XMODEM/CRC....
Ready to RECEIVE File xcode.bin in binary mode
Send several Control-X characters to cCKCKCKCKCKCKCK

XMODEM transfer complete, checking CRC....
Verified operational code CRC.
```

```
The following Enterasys Header is in the image:

MD5 Checksum.....................fe967970996c4c8c43a10cd1cd7be99a
Boot File Identifier............0x0517
Header Version..................0x0100
Image Type......................0x82
Image Offset....................0x004d
Image length....................0x006053b3
Ident Strings Length............0x0028
Ident Strings..................
    C2G124-24
C2G124-48
C2H124-48
C2K124_24
Image Version Length............0x7
Image Version Bytes.............0x30 0x2e 0x35 0x2e 0x30 0x2e 0x34 (0.5.0.4)
```

7. From the boot menu options screen, type **2** to display the baud rate selection screen again.
8. Type **4** set the switch baud rate to **9600**. The following message displays:

   ```
   Setting baud rate to 9600, you must change your terminal baud rate.
   ```

9. Set the terminal baud rate to **9600** and press ENTER.
10. From the boot menu options screen, type **1** to start the new operational code. The following message displays:

    ```
    Operational Code Date: Tue Jun 29 08:34:05 2004
    Uncompressing.....
    ```

Reverting to a Previous Image

In the event that you need to downgrade to a previous version of code, you can do so by completing the following steps as described in this chapter.

Caution: Before reverting to a previous image, always back up your configuration by saving it to a file (**show config outfile** on page 3-43). You can then copy the file to a remote location (**copy** on page 3-45).

Note: You will not be able to peform these steps remotely unless you have remote console support.

1. Save your running configuration with the **save config** command.
2. Make a copy of the current configuration with the **show config outfile configs/***filename* command. Use the **dir** command to confirm that the file was created.
3. If desired, copy the file to a remote TFTP server with the **copy** command:

   copy tftp://configs/*filename server_ipaddr/path and filename*

4. Load your previous version of code on the device, as described in "Downloading a Firmware Image" (page 3-32).
5. Set this older version of code to be the boot code with the set boot system command (page 3-36). When the system asks if you want to reset the device, specify no (**n**).
6. Reload the saved configuration onto the device with the **configure** command, described on page 3-44.

7. Reboot the system using the reset command (page 3-50).

Caution: If you do not follow the steps above, you may lose remote connectivity to the switch.

Reviewing and Selecting a Boot Firmware Image

Purpose

To display and set the image file the switch loads at startup. The C3 switch allows you to download and store a backup image, which can be selected as the startup image by using the commands described in this section.

Commands

For information about...	Refer to page...
show boot system	3-35
set boot system	3-36

show boot system

Use this command to display the firmware image the switch loads at startup.

Syntax

`show boot system`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the switch's boot firmware image:

```
C3(su)->show boot system
Current system image to boot: bootfile
```

set boot system

Use this command to set the firmware image the switch loads at startup.

Syntax

set boot system *filename*

Parameters

filename	Specifies the name of the firmware image file.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command allows you to set the firmware image to be loaded at startup. You can choose to reset the system to use the new firmware image immediately, or you can choose to only specify the new image to be loaded the next time the switch is rebooted.

You can use the **dir** command to display the "Active" image and the "Boot" image, which will be the image loaded at the next system reboot.

Note: If you are changing the firmware image to a version *earlier* than the current version, refer to "Reverting to a Previous Image" on page 3-34 for the correct steps to follow.

Example

This example shows how to set the boot firmware image file to be used at the next reboot of the system, by answering "n" to the prompt. The **dir** command is then executed to display the Active and Boot images.

```
C3(su)->set boot system c3_06.03.03.0007
This command can optionally reset the system to boot the new image.
Do you want to reset now (y/n) [n]?n

C3(su)->dir
Images:
=====================================================================
Filename:      c3_06.03.00.0026 (Active)
Version:        06.03.00.0026
Size:              9405440 (bytes)
Date:             Fri Jul 18 12:48:35 2008
CheckSum:    f1626ccf10d8f48cd6c3e79ab602342a
Compatibility: <platform specific>

Filename:      c3_06.03.03.0007 (Boot)
Version:        06.03.03.0007
Size:              8290304 (bytes)
Date:             Fri May  9 11:35:27 2008
CheckSum:    9f820d79239f10890442f8ff1f2bc914
Compatibility: <platform specific>
```

Starting and Configuring Telnet

Purpose

To enable or disable Telnet, and to start a Telnet session to a remote host. The SecureStack C3 switch allows a total of four inbound and / or outbound Telnet session to run simultaneously.

Commands

show telnet

Use this command to display the status of Telnet on the switch.

Syntax

show telnet

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display Telnet status:

```
C3(su)->show telnet
Telnet inbound is currently: ENABLED
Telnet outbound is currently: ENABLED
```

set telnet

Use this command to enable or disable Telnet on the switch.

Syntax

set telnet {**enable** | **disable**} [**inbound** | **outbound** | **all**]

Parameters

enable | **disable**	Enables or disables Telnet services.
inbound | **outbound** | **all**	(Optional) Specifies inbound service (the ability to Telnet to this switch), outbound service (the ability to Telnet to other devices), or all (both inbound and outbound).

Defaults

If not specified, both inbound and outbound Telnet service will be enabled.

Mode

Switch command, read-write.

Example

This example shows how to disable inbound and outbound Telnet services:

```
C3(su)->set telnet disable all
Disconnect all telnet sessions and disable now (y/n)? [n]: y
All telnet sessions have been terminated, telnet is now disabled.
```

telnet

Use this command to start a Telnet connection to a remote host. The SecureStack C3 switch allows a total of four inbound and / or outbound Telnet session to run simultaneously.

Syntax

telnet *host* [*port*]

Parameters

host	Specifies the name or IP address of the remote host.
port	(Optional) Specifies the server port number.

Defaults

If not specified, the default *port* number 23 will be used.

Mode

Switch command, read-write.

Example

This example shows how to start a Telnet session to a host at 10.21.42.13:

```
C3(su)->telnet 10.21.42.13
```

Managing Switch Configuration and Files

Configuration Persistence Mode

The default state of configuration persistence mode is "auto," which means that when CLI configuration commands are entered, or when a configuration file stored on the switch is executed, the configuration is saved to NVRAM automatically at the following intervals:

- On a standalone unit, the configuration is checked every two minutes and saved if there has been a change.
- On a stack, the configuration is saved across the stack every 30 minutes if there has been a change.

If you want to save a running configuration to NVRAM more often than the automatic intervals, execute the **save config** command and wait for the system prompt to return. After the prompt returns, the configuration will be persistent.

You can change the persistence mode from "auto" to "manual" with the **set snmp persistmode** command. If the persistence mode is set to "manual," configuration commands will not be automatically written to NVRAM. Although the configuration commands will actively modify the running configuration, they will not persist across a reset unless the **save config** command has been executed.

Note: When your device is configured for manual SNMP persistence mode, and you attempt to change the boot system image, the device will not prompt you to save changes or warn you that changes will be lost.

Purpose

To set and view the persistence mode for CLI configuration commands, manually save the running configuration, view, manage, and execute configuration files and image files, and set and view TFTP parameters.

Commands

For information about...	Refer to page...
show snmp persistmode	3-40
set snmp persistmode	3-40
save config	3-41
dir	3-41
show file	3-42
show config	3-43
configure	3-44
copy	3-45
delete	3-46
show tftp settings	3-46
set tftp timeout	3-47

For information about...	Refer to page...
clear tftp timeout	3-47
set tftp retry	3-48
clear tftp retry	3-48

show snmp persistmode

Use this command to display the configuration persistence mode setting.

Syntax

show snmp persistmode

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Usage

By default, the mode is set to "auto save," which automatically saves configuration changes at specific intervals. If the mode is set to "manual," configuration commands are never automatically saved. In order to make configuration changes persistent when the mode is manual, the **save config** command must be issued as described in "Configuration Persistence Mode" on page 3-39.

Example

This example shows how to display the configuration persistence mode setting. In this case, persistence mode is set to "manual", which means configuration changes are not being automatically saved.

```
C3(su)->show snmp persistmode
persistmode is manual
```

set snmp persistmode

Use this command to set the configuration persistence mode, which determines whether user-defined configuration changes are saved automatically, or require issuing the **save config** command. See "Configuration Persistence Mode" on page 3-39 for more information.

Syntax

set snmp persistmode {**auto** | **manual**}

Parameters

auto	Sets the configuration persistence mode to automatic. This is the default state.
manual	Sets the configuration persistence mode to manual. In order to make configuration changes persistent, the **save config** command must be issued as described in "save config" on page 3-41. This mode is useful for reverting back to old configurations.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the configuration persistence mode to manual:

```
C3(su)->set snmp persistmode manual
```

save config

Use this command to save the running configuration. If applicable, this command will save the configuration to all switch members in a stack.

Syntax

```
save config
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to save the running configuration:

```
C3(su)->save config
```

dir

Use this command to list configuration and image files stored in the file system.

Syntax

```
dir [filename]
```

Parameters

filename	(Optional) Specifies the file name or directory to list.

Defaults

If **filename** is not specified, all files in the system will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to list all the configuration and image files in the system. The display indicates which image file is the Active file and which image file is the Boot file that will be used the next time the system reboots.

```
C3(su)->dir
Images:
========================================================================
Filename:      c3-series_06.03.00.0029 (Active)
Version:       06.03.00.0029
Size:          9411584 (bytes)
Date:          Fri Aug  1 06:55:23 2008
CheckSum:      6126a7aadfdf05150afb6eca51982302
Compatibility: <platform specific>

Filename:      c3-series_06.03.00.0030 (Boot)
Version:       06.03.00.0030
Size:          9411584 (bytes)
Date:          Fri Aug  8 08:44:04 2008
CheckSum:      627938b785fa7fdb8eed74672af1edcc
Compatibility: <platform specific>

Files:                          Size
=============================== ========
configs:
base_may                        22629
base_apr                        22629
base_july                       20581
base_june                       20581
logs:
current.log                     2065
```

show file

Use this command to display the contents of a file.

Syntax

show file *filename*

Parameters

filename	Specifies the name of the file to display.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display a text file named "myconfig" in the configs/ directory. Note that only a portion of the file is shown in this example.

```
C3(rw)->show file configs/myconfig
...
17 : #snmp
18 :
19 : set snmp access ro security-model v1 exact read All notify All nonvolatile
20 :
21 : set snmp access ro security-model v2c exact read All notify All nonvolatile
22 :
23 : set snmp access public security-model v1 exact read All write All notify All
nonvolatile
24 :
25 : set snmp access public security-model v2c exact read All write All notify All
nonvolatile
26 :
27 : set snmp access public security-model usm exact read All write All notify All
nonvolatile
28 :
29 : set snmp community :xxxxxxxxxxx:
30 :
31 : set snmp group ro user ro security-model v1
32 :
33 : set snmp group public user public security-model v1
34 :
35 : set snmp group ro user ro security-model v2c
36 :
37 : set snmp group public user public security-model v2c
38 :
39 : set snmp group public user public security-model usm
40 :
41 : set snmp user public authentication md5 :xxxxxxxxx: encryption des privacy
:xxxxxxxxxx:
42 :
43 : set snmp view viewname All subtree 1
44 :
45 : !
```

show config

Use this command to display the system configuration or write the configuration to a file.

Syntax

show config [**all** | *facility*] [**outfile** {**configs/***filename*}]

Parameters

all	(Optional) Displays default and non-default configuration settings.
facility	(Optional) Specifies the exact name of one facility for which to show configuration. For example, enter "router" to show only router configuration.
outfile	(Optional) Specifies that the current configuration will be written to a text file in the configs/ directory.
configs/*filename*	Specifies a filename in the configs/ directory to display.

Defaults

By default, **show config** will display all non-default configuration information for all facilities.

Mode

Switch command, read-only.

Usage

The separate facilities that can be displayed by this command are identified in the display of the current configuration by a # preceding the facility name. For example, "#port" indicates the facility name "port."

Examples

This example shows how to write the current configuration to a file named save_config2:

```
C3(rw)->show config all outfile configs/save_config2
```

This example shows how to display configuration for the facility "port".

```
C3(rw)->show config port
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.

begin
!
#***** NON-DEFAULT CONFIGURATION *****
!
!

#port
set port jumbo disable ge.1.1

!
end
```

configure

Use this command to execute a previously downloaded configuration file stored on the switch.

Syntax

configure *filename* [**append**]

Parameters

filename	Specifies the path and file name of the configuration file to execute.
append	(Optional) Appends the configuration file contents to the current configuration. This is equivalent to typing the contents of the config file directly into the CLI and can be used, for example, to make incremental adjustments to the current configuration.

Defaults

If **append** is not specified, the current running configuration will be replaced with the contents of the configuration file, which will require an automated reset of the chassis.

Mode

Switch command, read-write.

Example

This example shows how to execute the "Jan1_2004.cfg" configuration file:

```
C3(su)->configure configs/Jan1_2004.cfg
```

copy

Use this command to upload or download an image or a CLI configuration file.

Syntax

copy *source* {*destination* | **system:image**}

Parameters

source	Specifies location and name of the source file to copy. Options are a local file path in the configs or logs directory, or the URL of a TFTP, Secure FTP (SFTP), or Secure Copy (SCP) server.
destination	Specifies location and name of the destination where the file will be copied. Options are a local file path in the configs directory, or the URL of a TFTP, SFTP, or SCP server.
system:image	The required destination of an image file. **Note:** Only TFTP can be used to download an image file.

Defaults

None.

Mode

Switch command, read-write.

Usage

SFTP and SCP can only be used to transfer configuration files or the logs/current.log file. You cannot use SFTP or SCP to download images (**system:image**).

Examples

This example shows how to download an image via TFTP:

```
C3(su)->copy tftp://10.1.192.34/version01000 system:image
```

This example shows how to download a configuration file to the configs directory:

```
C3(su)->copy tftp://10.1.192.1/Jan1_2004.cfg configs/Jan1_2004.cfg
```

This example shows how to upload a configuration file from the configs directory using SFTP.

```
C3(su)->copy configs/Jan1_2009.cfg sftp://user:passwd@10.1.192.1/Jan1_2009.cfg
```

delete

Use this command to remove an image or a CLI configuration file from the switch.

Syntax

delete *filename*

Parameters

filename	Specifies the local path name to the file. Valid directories are /images and /configs.44.

Defaults

None.

Mode

Switch command, read-write.

Usage

Use the dir command (page 3-41) to display current image and configuration file names.

Example

This example shows how to delete the “Jan1_2004.cfg” configuration file:

```
C3(su)->delete configs/Jan1_2004.cfg
```

show tftp settings

Use this command to display TFTP settings used by the switch during data transfers using TFTP.

Syntax

show tftp settings

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Usage

The TFTP timeout value can be set with the **set tftp timeout** command. The TFTP retry value can be set with the **set tftp retry** command.

Example

This example shows the output of this command.

```
C3(ro)->show tftp settings
TFTP packet timeout (seconds): 2
TFTP max retry: 5
```

set tftp timeout

Use this command to configure how long TFTP will wait for a reply of either an acknowledgement packet or a data packet during a data transfer.

Syntax

set tftp timeout *seconds*

Parameters

seconds	Specifies the number of seconds to wait for a reply. The valid range is from 1 to 30 seconds. Default value is 2 seconds.

Defaults

None.

Mode

Switch command, read-write.

Example

This example sets the timeout period to 4 seconds.

```
C3(rw)->set tftp timeout 4
```

clear tftp timeout

Use this command to reset the TFTP timeout value to the default value of 2 seconds.

Syntax

clear tftp timeout

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the timeout value to the default of 2 seconds.

```
C3(rw)-> clear tftp timeout
```

set tftp retry

Use this command to configure how many times TFTP will resend a packet, either an acknowledgement packet or a data packet.

Syntax

set tftp retry *retry*

Parameters

retry	Specifies the number of times a packet will be resent. The valid range is from 1 to 1000. Default value is 5 retries.

Defaults

None.

Mode

Switch command, read-write.

Example

This example sets the retry count to 3.

```
C3(rw)->set tftp retry 3
```

clear tftp retry

Use this command to reset the TFTP retry value to the default value of 5 retries.

Syntax

clear tftp retry

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the retry value to the default of 5 retries.

```
C3(rw)-> clear tftp retry
```

Clearing and Closing the CLI

Purpose

To clear the CLI screen or to close your CLI session.

Commands

For information about...	Refer to page...
cls	3-49
exit	3-50

cls (clear screen)

Use this command to clear the screen for the current CLI session.

Syntax

`cls`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to clear the CLI screen:

```
C3(su)->cls
```

exit

Use either of these commands to leave a CLI session.

Syntax

exit

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Usage

By default, switch timeout occurs after 15 minutes of user inactivity, automatically closing your CLI session. Use the set logout command (page 3-30) to change this default.

Example

This example shows how to exit a CLI session:

```
C3(su)->exit
```

Resetting the Switch

Purpose

To reset one or more switches, and to clear the user-defined configuration parameters.

Commands

For information about...	Refer to page...
reset	3-50
clear config	3-51

reset

Use this command to reset the switch without losing any user-defined configuration settings.

Syntax

reset [*unit*]

Parameters

unit	(Optional) Specifies a unit to be reset.

Defaults

If no *unit* ID is specified, the entire system will be reset.

Mode

Switch command, read-write.

Usage

A SecureStack C3 switch can also be reset with the RESET button located on its front panel. For information on how to do this, refer to the SecureStack C3 Installation Guide shipped with your switch.

Examples

This example shows how to reset the system:

```
C3(su)->reset
Are you sure you want to reload the stack? (y/n) y

Saving Configuration to stacking members
Reloading all switches.
```

This example shows how to reset unit 1:

```
C3(su)->reset 1
Are you sure you want to reload the switch? (y/n) y

Reloading switch 1.
This switch is manager of the stack.
STACK: detach 3 units
```

clear config

Use this command to clear the user-defined configuration parameters.

Syntax

clear config [**all**]

Parameters

all	(Optional) Clears user-defined configuration parameters (and stack unit numbers and priorities, if applicable).

Defaults

If **all** is not specified, stacking configuration parameters will not be cleared.

Mode

Switch command, read-write.

Usage

When using the **clear config** command to clear configuration parameters in a stack, it is important to remember the following:

- Use **clear config** to clear configuration parameters without clearing stack unit IDs. This command WILL NOT clear stack parameters and avoids the process of re-numbering the stack.
- Use **clear config all** when it is necessary to clear all configuration parameters, including stack unit IDs (if applicable) and switch priority values.
- Use the **clear ip address** command to clear the IP address.

Configuration parameters and stacking information can also be cleared on the master unit only by selecting option 10 (restore configuration to factory defaults) from the boot menu on switch startup. This selection will leave stacking priorities on all other units, if applicable.

Example

This example shows how to clear configuration parameters (including stacking parameters, if applicable):

```
C3(su)->clear config all
```

Using and Configuring WebView

Purpose

By default, WebView (The Enterasys Networks embedded web server for switch configuration and management tasks) is enabled on TCP port number 80 on the SecureStack C3 switch. You can verify WebView status, and enable or disable WebView using the commands described in this section. WebView can also be securely used over SSL port 443, if SSL is enabled on the switch. By default, SSL is disabled.

To use WebView, type the IP address of the switch in your browser. To use WebView over SSL, type in https:// then the IP address of the switch. For example, https://172.16.2.10.

Commands

For information about...	Refer to page...
show webview	3-52
set webview	3-53
show ssl	3-53
set ssl	3-54

show webview

Use this command to display WebView status.

Syntax

show webview

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display WebView status:

```
C3(rw)->show webview
WebView is Enabled.
```

set webview

Use this command to enable or disable WebView on the switch.

Syntax

set webview {**enable** | **disable**}

Parameters

enable | **disable**	Enable or disable WebView on the switch.

Defaults

None.

Mode

Switch command, read-write.

Usage

It is good practice for security reasons to disable HTTP access on the switch when finished configuring with WebView, and then to only enable WebView on the switch when changes need to be made.

Example

This example shows how to disable WebView on the switch:

```
C3(rw)->set webview disable
```

show ssl

Use this command to display SSL status.

Syntax

show ssl

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display SSL status:

```
C3(rw)->show ssl
SSL status: Enabled
```

set ssl

Use this command to enable or disable the use of WebView over SSL port 443. By default, SSL is disabled on the switch. This command can also be used to reinitialize the hostkey that is used for encryption.

Syntax

set ssl {**enabled** | **disabled** | **reinitialize** | **hostkey reinitialize**}

Parameters

enabled | **disabled**	Enables or disables the ability to use WebView over SSL.
reinitialize	Stops and then restarts the SSL process.
hostkey reinitialize	Stops SSL, regenerates new keys, and then restarts SSL.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to enable SSL:

```
C3(rw)->set ssl enabled
```

Gathering Technical Support Information

Purpose

To gather common technical support information.

Command

For information about...	Refer to page...
show support	3-55

show support

Use this command to display switch information for troubleshooting.

Syntax

show support

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Usage

This command initiates a number of **show** commands to easily gather basic information from an installed device. To use this command, set your console to capture the output to a file first, before executing the command, since the output is extensive.

Output from the following commands is gathered by this command:

- show version
- show logging buffer
- show port status
- show system utilization process
- show system utilization storage
- show config

Example

There is no display example because the output of this command is quite lengthy.

Configuring Hostprotect

Purpose

This feature enables rate limiting of host bound traffic on SecureStack C3 switches, to assist in the prevention of Denial of Service issues. When enabled, the hostprotect functionality applies a 64 kbps meter to control plane traffic, such as BPDUs or LACP packets, destined for the host processor.

Commands

show system hostprotect

Use this command to display the status of the hostprotect feature.

Syntax

```
show system hostprotect
```

Parameters

None.

Defaults

Hostprotect is enabled by default.

Mode

Switch command, read-only.

Example

This example shows the output of this command.

```
C3(rw)->show system hostprotect
hostprotect Enable
```

set system hostprotect

Use this command to enable or disable hostprotect on the switch.

Syntax

```
set system hostprotect {enable | disable}
```

Parameters

enable	Enables hostprotect mode.
disable	Disables hostprotect mode.

Defaults

This feature is disabled by default.

Mode

Switch command, read-write.

Usage

Hostprotect uses hardware resources that are also used for priority queues (see "Configuring Priority to Transmit Queue Mapping" on page 12-4), so if hostprotect is enabled, priority queues are limited.

At boot time, if more than two priority queue mappings are defined, in addition to the default mapping, hostprotect will be disabled.

At run time, if hostprotect if enabled, and you attempt to define more than two priority queue mappings (with the **set port priority-queue** command), the set will fail and a warning message will be displayed.

At run time, if more than two priority queue mappings exist, and you attempt to enable hostprotect with this command, the set will fail and a warning message will be displayed.

Changing the hostprotect status requires a reset of the switch or stack of switches.

Example

This example disables hostprotect.

```
C3(rw)->set system hostprotect disable

Changes in the host protect mode will require resetting this stack.
Are you sure you want to continue? (y/n)y
```

clear system hostprotect

Use this command to return the hostprotect status to the default of enabled.

Syntax

```
clear system hostprotect
```

Parameters

None.

Defaults

The default state is enabled.

Mode

Switch command, read-write.

Usage

Changing the hostprotect status requires a reset of the switch or stack of switches. If more than two priority queue mappings exist and you execute this command to reset the hostprotect status to enabled, the command will not complete and you will get a warning message.

Example

This example attempts to return the hostprotect status to the default, but the command cannot complete because more than two priority queue mappings exist.

```
C3(rw)->clear system hostprotect

Changes in the host protect mode will require resetting this stack.
Are you sure you want to continue? (y/n)y

Error: Could not set system host protect to default
```

4

Activating Licensed Features

In order to enable the C3 advanced features, such as Advanced Routing, you must purchase and activate a license key. If you have purchased a license, you can proceed to activate your license as described in this section. If you wish to obtain a permanent or evaluation license, use the Enterasys Customer Portal or contact the Enterasys Networks Sales Department.

Note: All members of a stack must be licensed in order to support licensed features in a stack environment. If the master unit in a stack has an activated license, all member units also must have an activated license in order to operate. If the master unit in a stack does not have an activated license, then the licensed functionality will not be available to member units, even if they have licenses installed.

License Key Field Descriptions

When Enterasys supplies a license, it will be sent to you as a character string similar to the following:

```
INCREMENT advrouter 2006.0127 27-jan-2011 0123456789AB 0123456789AB
```

The contents of the six fields, from the left, indicate:

- Type—the type of license. For the SecureStack C3, the value in this field is always "INCREMENT."
- Feature—description of the feature being licensed. For example, "advrouter" as shown in the character string above.
- Date-based version (DBV)—a date-related string. For the SecureStack C3, the value in this field is not significant.
- Expiration type—indicates whether the license is a permanent or an evaluation license. If the license is an evaluation license, this field will contain the expiration date of the license. If the license is a permanent license, this field will contain the word "permanent."
- Key—the license key.
- Host ID—the serial number of the switch to which this license applies.

When activating licenses on SecureStack devices, we recommend that you copy and paste the license character string, rather than entering the text manually.

Licensing Procedure in a Stack Environment

The licenses for all members of an operating stack can be activated during a single CLI session, by following these steps:

1. Obtain valid licenses for all members of the stack from the Enterasys Customer Portal.

2. Optionally, note the serial numbers of the switches in the stack. You can use the **show system hardware** command (page 3-14) to display the switch serial numbers.

Note: Since license keys are applied to the correct stack member switch automatically, based on the switch serial number that is part of the license string, you should know the serial numbers of the switches in order to enable the licenses of the member switches first, before the master unit.

3. Enable the licenses on the stack members first, before enabling the master unit, using the **set license** command (page 4-3). For example:

```
C3(rw)->set license INCREMENT advrouter 2006.0127 27-jan-2011 0123456789AB
0123456789AB
```

4. Enable the license on the switch master unit last, using the **set license** command.

Adding a New Member to a Licensed Stack

When a SecureStack C3 switch without a license is added to a stack that has licensing enabled, the ports on the new switch will not pass traffic until a license has been applied to the new switch. To add a new member to a licensed stack:

1. Obtain a license for the new switch from the Enterasys Customer Portal.
2. Add the new unit to the stack, following the procedure in "Adding a New Unit to an Existing Stack" on page 2-3.
3. Use the **set license** command to install and activate the new switch's license. The new switch will then join the stack and its ports will be attached.

Alternatively, you can install and activate the new switch's license first, before adding the switch to the stack.

Clearing, Showing, and Applying Licenses

Licenses can be displayed, applied, and cleared only with the license commands described in this chapter. General configuration commands such as **show config** or **clear config** do not apply to licenses.

Every license is associated with a specific hardware platform, based on the serial number of the hardware platform. If you need to move a license from one hardware platform to another, you must contact Enterasys Customer Support to arrange for re-hosting of the license.

Commands

For information about...	Refer to page...
set license	4-3
show license	4-4
clear license	4-4

set license

Use this command to activate the SecureStack C3 licensed features.

Syntax

set license *type feature DBV expiration key hostid*

Parameters

type	Specifies the type of license. For the SecureStack C3, the value in this field is always INCREMENT.
feature	The name of the feature being licensed.
DBV	A date-related string generated as part of the license.
expiration	Indicates whether the license is a permanent or an evaluation license. If the license is an evaluation license, this field will contain the expiration date of the license. If the license is a permanent license, this field will contain the word "permanent."
key	The license key.
hostid	The serial number of the switch to which this license applies.

Defaults

None.

Mode

Switch command, read-write.

Usage

If multiple switches are used in a stack, an individual license is required for each stack member. Refer to "Licensing Procedure in a Stack Environment" on page 4-1 for more information.

When activating licenses with this command, Enterasys Networks recommends that you copy and paste the entire license character string, rather than enter the text manually. If you enter the character string manually, ensure that you exactly match the capitalization of the character string sent to you.

Every license is associated with a specific hardware platform, based on the serial number of the hardware platform. If you need to move a license from one hardware platform to another, you must contact Enterasys Customer Support to arrange for re-hosting of the license.

Example

This example shows how to activate a permanent license key on the switch with serial number `075103099041`. In this example, the switch is a stand-alone unit so its unit number is 1.

```
C3(rw)->set license INCREMENT advrouter 2008.0212 permanent DF6A8558E5AB
075103099041
Validating license on unit 1
License successfully validated and set on unit 1
C3(rw)->
```

show license

Use this command to display license key information for switches with activated licenses.

Syntax

show license [**unit** *number*]

Parameters

unit *number*	(Optional) Specifies the switch for which to display license information. Refer to Chapter 2, **Configuring Switches in a Stack**, for more information about stack unit IDs, or numbers.

Defaults

If no unit number is specified, license key information for all switches in the stack is displayed.

Mode

Switch command, read-only.

Usage

Licenses can be displayed, applied, and cleared only with the license commands described in this chapter. General configuration commands such as **show config** or **clear config** do not affect licenses.

Example

This example shows how to display license key information for switch unit 1 in the stack.

```
C3(ro)->show license unit 1
unit 1
key: INCREMENT advrouter 2006.0728 permanent 31173CAC6495 045100039001
status: Active
```

clear license

Use this command to clear the license key settings..

Syntax

clear license featureId *feature*

Parameters

featureID *feature*	The name of the feature being cleared.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the `advrouter` licensed feature :

```
C3(rw)->clear license featureId advrouter
```

5

Configuring System Power and PoE

Important Notice

The commands in this section apply only to PoE-equipped devices. Consult the Installation Guide for your product to determine if it is PoE-equipped.

The commands in this chapter allow you to review and set system power and PoE (Power over Ethernet) parameters, including the power available to the system, the usage threshold for each module, whether or not SNMP trap messages will be sent when power status changes, and per-port PoE settings.

Commands

show inlinepower

Use this command to display system power properties.

Syntax

```
show inlinepower
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display system power properties:

```
C3(su)->show inlinepower
Detection Mode         : auto

Unit  Status   Power(W)   Consumption(W)   Usage(%)   Threshold(%)   Trap
----  ------   --------   --------------   --------   ------------   ----
1     auto     375         0.00            0.00       80             enable
```

Table 5-1 provides an explanation of the command output.

Table 5-1 show inlinepower Output Details

Output	What It Displays...
Detection Mode	Displays the PD detection mode used by the switch. The detection mode can be configured with the command "set inlinepower detectionmode" (page 5-3).
Unit	Number of PoE-capable module.
Status	Whether the PoE administrative state is off (disabled) or auto (on). This state is not configurable.
Power (W)	Unit's available power wattage.
Consumption (W)	Unit's power wattage consumed.
Usage (%)	Unit's percentage of total system PoE power usage.
Threshold (%)	Unit's alloted percentage of total PoE power available in the system. The threshold can be configured with the command "set inlinepower threshold" (page 5-2).
Trap	Whether PoE trap messaging is enabled or disabled on this unit. Trap messaging can be configured with the command "set inlinepower trap" (page 5-3).

set inlinepower threshold

Use this command to set the power usage threshold on a specified unit or module.

Syntax

`set inlinepower threshold` *`usage-threshold module-number`*

Parameters

usage-threshold	Specifies a power threshold as a percentage of available system power. Valid values are **11** to **100**.
module-number	Specifies the module or unit on which to set the power threshold.

Defaults

None.

Mode

Switch command, read-write.

Usage

The threshold is expressed as a percentage of the available PoE power. When this threshold is reached, a trap will be sent if traps are enabled with the set inlinepower trap command.

Example

This example shows how to set the power threshold to 90 on module/unit 1:

```
C3(su)->set inlinepower threshold 90 1
```

set inlinepower trap

Use this command to enable or disable the sending of an SNMP trap message for a unit or module whenever the status of its ports changes, or whenever the unit's power usage threshold is crossed.

Syntax

set inlinepower trap {**disable** | **enable**} *module-number*

Parameters

disable | **enable**	Disables or enables inline power trap messaging.
module-number	Specifies the module or unit on which to disable or enable trap messaging.

Defaults

Sending of traps is disabled by default.

Mode

Switch command, read-write.

Usage

The module's or unit's power usage threshold must be set using the **set inlinepower threshold** command as described on page 5-2.

Example

This example shows how to enable inline power trap messaging on module 1:

```
C3(su)->set inlinepower trap enable 1
```

set inlinepower detectionmode

Use this command to specify the method the switch will use to detect PDs (powered devices) connected to its ports.

Syntax

set inlinepower detectionmode {**auto** | **ieee**)

Parameters

auto	Specifies that the switch will use the standard 802.3af detection method first. If that fails, then the switch will use the legacy (pre 802.3af standard) capacitance method of detection.
ieee	Specifies that the switch will only use the standard 802.3af detection method.

Defaults

Default detection mode is **auto**.

Mode

Switch command, read-write.

Usage

This command is used to specify how the switch should detect PDs connected to its ports. The PoE hardware in the switches can use the IEEE standard 802.3af (resistor-based) method or a proprietary method using capacitor detection.

If **auto** is configured, the switch will first use the IEEE resistor-based detection method, and if that fails, the switch will use the capacitor-based detection method. If **ieee** is configured, only the IEEE resistor-based detection method will be used.

Example

This example sets the switch's PD detection mode to IEEE standard 802.3af only.

```
C3(su)->set inlinepower detectionmode ieee
```

show port inlinepower

Use this command to display all ports supporting PoE.

Syntax

show port inlinepower [*port-string*]

Parameters

port-string	(Optional) Displays information for specific PoE port(s).

Defaults

If not specified, information for all PoE ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display PoE information for port `ge.2.1`. In this case, the port's administrative state, PoE priority and class have not been changed from default values:

```
C3(su)->show port inlinepower ge.2.1
Port     Type      Admin   Oper        Priority      Class       Power(W)
----     ----      -----   ----        --------      -----       --------
ge.2.1   wireless  auto    searching   low           0           15.4
```

set port inlinepower

Use this command to configure PoE parameters on one or more ports.

Syntax

set port inlinepower *port-string* {[**admin** {**off** | **auto**}] [**priority** {**critical** | **high** | **low**}] [**type** *type*]}

Parameters

port-string	Specifies the port(s) on which to configure PoE.
admin off | **auto**	Sets the PoE administrative state to off (disabled) or auto (on).
priority critical | **high** | **low**	Sets the port(s) priority for the PoE allocation algorithm to critical (highest), high or low.
type *type*	Specifies a string describing the type of device connected to a port.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to enable PoE on port ge.3.1 with critical priority:

```
C3(su)->set port inlinepower ge.3.1 admin auto priority critical
```

6

Discovery Protocol Configuration

This chapter describes how to configure discovery protocols. For more extensive configuration information, refer to the "Configuring Neighbor Discovery" feature guide on the Enterasys Networks web site: http://www.enterasys.com/support/manuals

Configuring CDP

Purpose

To review and configure the Enterasys CDP discovery protocol. This protocol is used to discover network topology. When enabled, this protocol allows Enterasys devices to send periodic PDUs about themselves to neighboring devices.

Commands

The commands used to review and configure the CDP discovery protocol are listed below.

show cdp

Use this command to display the status of the CDP discovery protocol and message interval on one or more ports.

Syntax

show cdp [*port-string*]

Parameters

port-string	(Optional) Displays CDP status for a specific port. For a detailed description of possible port-string values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, all CDP information will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display CDP information for ports ge.1.1 through ge.1.9:

```
C3(su)->show cdp ge.1.1-9
CDP Global Status          :auto-enable
CDP Version Supported      :30 hex
CDP Hold Time              :180
CDP Authentication Code    :00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 hex
CDP Transmit Frequency     :60

Port       Status
-----------------
ge.1.1     auto-enable
ge.1.2     auto-enable
ge.1.3     auto-enable
ge.1.4     auto-enable
ge.1.5     auto-enable
ge.1.6     auto-enable
ge.1.7     auto-enable
ge.1.8     auto-enable
ge.1.9     auto-enable
```

Table 6-1 provides an explanation of the command output.

Table 6-1 show cdp Output Details

Output Field	What It Displays...
CDP Global Status	Whether CDP is globally auto-enabled, enabled or disabled. The default state of auto-enabled can be reset with the set cdp state command. For details, refer to "set cdp state" on page 6-3.
CDP Versions Supported	CDP version number(s) supported by the switch.
CDP Hold Time	Minimum time interval (in seconds) at which CDP configuration messages can be set. The default of 180 seconds can be reset with the set cdp hold-time command. For details, refer to "set cdp hold-time" on page 6-5.

Table 6-1 show cdp Output Details (Continued)

Output Field	What It Displays...
CDP Authentication Code	Authentication code for CDP discovery protocol. The default of 00-00-00-00-00-00-00-00 can be reset using the set cdp auth command. For details, refer to "set cdp auth" on page 6-4.
CDP Transmit Frequency	Frequency (in seconds) at which CDP messages can be transmitted. The default of 60 seconds can be reset with the set cdp interval command. For details, refer to "set cdp interval" on page 6-4.
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
Status	Whether CDP is enabled, disabled or auto-enabled on the port.

set cdp state

Use this command to enable or disable the CDP discovery protocol on one or more ports.

Syntax

```
set cdp state {auto | disable | enable} [port-string]
```

Parameters

auto | **disable** | **enable**	Auto-enables, disables or enables the CDP protocol on the specified port(s). In auto-enable mode, which is the default mode for all ports, a port automatically becomes CDP-enabled upon receiving its first CDP message.
port-string	(Optional) Enables or disables CDP on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, the CDP state will be globally set.

Mode

Switch command, read-write.

Examples

This example shows how to globally enable CDP:

```
C3(su)->set cdp state enable
```

This example shows how to enable the CDP for port ge.1.2:

```
C3(su)->set cdp state enable ge.1.2
```

This example shows how to disable the CDP for port ge.1.2:

```
C3(su)->set cdp state disable ge.1.2
```

set cdp auth

Use this command to set a global CDP authentication code.

Syntax

set cdp auth *auth-code*

Parameters

auth-code	Specifies an authentication code for the CDP protocol. This can be up to 16 hexadecimal values separated by commas.

Defaults

None.

Mode

Switch command, read-write.

Usage

The authentication code value determines a switch's CDP domain. If two or more switches have the same CDP authentication code, they will be entered into each other's CDP neighbor tables. If they have different authentication codes, they are in different domains and will not be entered into each other's CDP neighbor tables.

A switch with the default authentication code (16 null characters) will recognize all switches, no matter what their authentication code, and enter them into its CDP neighbor table.

Example

This example shows how to set the CDP authentication code to 1,2,3,4,5,6,7,8:

```
C3(su)->set cdp auth 1,2,3,4,5,6,7,8:
```

set cdp interval

Use this command to set the message interval frequency (in seconds) of the CDP discovery protocol.

Syntax

set cdp interval *frequency*

Parameters

frequency	Specifies the transmit frequency of CDP messages in seconds.Valid values are from 5 to 900 seconds.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the CDP interval frequency to 15 seconds:

```
C3(su)->set cdp interval 15
```

set cdp hold-time

Use this command to set the hold time value for CDP discovery protocol configuration messages.

Syntax

set cdp hold-time *hold-time*

Parameters

hold-time	Specifies the hold time value for CDP messages in seconds.Valid values are from 15 to 600.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set CDP hold time to 60 seconds:

```
C3(su)->set cdp hold-time 60
```

clear cdp

Use this command to reset CDP discovery protocol settings to defaults.

Syntax

clear cdp {[**state**] [**port-state** *port-string*] [**interval**] [**hold-time**] [**auth-code**]}

Parameters

state	(Optional) Resets the global CDP state to auto-enabled.
port-state *port-string*	(Optional) Resets the port state on specific port(s) to auto-enabled.
interval	(Optional) Resets the message frequency interval to 60 seconds.
hold-time	(Optional) Resets the hold time value to 180 seconds.
auth-code	(Optional) Resets the authentication code to 16 bytes of 00 (00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00).

Defaults

At least one optional parameter must be entered.

Mode

Switch command, read-write.

Example

This example shows how to reset the CDP state to auto-enabled:

```
C3(su)->clear cdp state
```

show neighbors

This command displays Neighbor Discovery information for either the CDP or Cisco DP protocols.

Syntax

show neighbors [*port-string*]

Parameters

port-string	(Optional) Specifies the port or ports for which to display Neighbor Discovery information.

Defaults

If no port is specified, all Neighbor Discovery information is displayed.

Mode

Switch command, read-only.

Usage

This command displays information discovered by both the CDP and the Cisco DP protocols.

Example

This example displays Neighbor Discovery information for all ports.

```
C3(su)->show neighbors

 Port       Device ID            Port ID           Type       Network Address
--------------------------------------------------------------------------------
ge.1.1      00036b8b1587         12.227.1.176      ciscodp    12.227.1.176
ge.1.6      0001f496126f         140.2.3.1         ciscodp    140.2.3.1
ge.1.6      00-01-f4-00-72-fe    140.2.4.102       cdp        140.2.4.102
ge.1.6      00-01-f4-00-70-8a    140.2.4.104       cdp        140.2.4.104
ge.1.6      00-01-f4-c5-f7-20    140.2.4.101       cdp        140.2.4.101
ge.1.6      00-01-f4-89-4f-ae    140.2.4.105       cdp        140.2.4.105
ge.1.6      00-01-f4-5f-1f-c0    140.2.1.11        cdp        140.2.1.11
ge.1.19     0001f400732e         165.32.100.10     ciscodp    165.32.100.10
```

Configuring Cisco Discovery Protocol

Purpose

To review and configure the Cisco discovery protocol. Discovery protocols are used to discover network topology. When enabled, they allow Cisco devices to send periodic PDUs about themselves to neighboring devices. Specifically, this feature enables recognizing PDUs from Cisco phones. A table of information about detected phones is kept by the switch and can be queried by the network administrator.

Commands

The commands used to review and configure the Cisco discovery protocol are listed below. Refer also to "show neighbors" on page 6-6.

show ciscodp

Use this command to display global Cisco discovery protocol information.

Syntax

```
show ciscodp
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display global Cisco DP information.

```
C3(su)->show ciscodp
CiscoDP :Enabled
Timer :5
Holdtime (TTl): 180
```

```
Device ID : 001188554A60
Last Change : WED NOV 08 13:19:56 2006
```

Table 6-2 provides an explanation of the command output.

Table 6-2 show ciscodp Output Details

Output Field	What It Displays...
CiscoDP	Whether Cisco DP is globally enabled or disabled. Auto indicates that Cisco DP will be globally enabled only if Cisco DP PDUs are received. Default setting of auto-enabled can be reset with the **set ciscodp status** command.
Timer	The number of seconds between Cisco discovery protocol PDU transmissions. The default of 60 seconds can be reset with the **set ciscodp timer** command.
Holdtime	Number of seconds neighboring devices will hold PDU transmissions from the sending device. Default value of 180 can be changed with the **set ciscodp holdtime** command.
Device ID	The MAC address of the switch.
Last Change	The time that the last Cisco DP neighbor was discovered.

show ciscodp port info

Use this command to display summary information about the Cisco discovery protocol on one or more ports.

Syntax

show ciscodp port info [*port-string*]

Parameters

port-string	(Optional) Displays Cisco DP information for a specific port. For a detailed description of possible port-string values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, Cisco DP information for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display Cisco DP information for Gigabit Ethernet port 1 in slot 1.

```
C3(su)->show ciscodp port info ge.1.1

 port       state      vvid      trusted   cos
-----------------------------------------------
ge.1.1     enable     none         yes      0
```

Table 6-3 provides an explanation of the command output.

Table 6-3 show ciscodp port info Output Details

Output Field	What It Displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
State	Whether Cisco DP is enabled, disabled or auto-enabled on the port. Default state of enabled can be changed using the **set ciscodp port** command.
vvid	Whether a voice VLAN ID has been set on this port. Default of none can be changed using the **set ciscodp port** command.
trusted	The trust mode of the port. Default of trusted can be changed using the **set ciscodp port** command.
cos	The Class of Service priority value for untrusted traffic. The default of 0 can be changed using the **set ciscodp port** command.

set ciscodp status

Use this command to enable or disable the Cisco discovery protocol globally on the switch.

Syntax

set ciscodp state {**auto** | **disable** | **enable**}

Parameters

auto	Globally enable only if Cisco DP PDUs are received.
disable	Globally disable Cisco discovery protocol.
enable	Globally enable Cisco discovery protocol.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to globally enable CiscoDP:

```
C3(su)->set ciscodp state enable
```

set ciscodp timer

Use this command to set the number of seconds between Cisco discovery protocol PDU transmissions.

Syntax

set ciscodp timer *seconds*

Parameters

seconds	Specifies the number of seconds between Cisco DP PDU transmissions. Valid values are from 5 to 254 seconds.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the Cisco DP timer to 120 seconds.

```
C3(su)->set ciscodp timer 120
```

set ciscodp holdtime

Use this command to set the time to live (TTL) for Cisco discovery protocol PDUs. This is the amount of time, in seconds, neighboring devices will hold PDU transmissions from the sending device.

Syntax

set ciscodp holdtime *hold-time*

Parameters

hold-time	Specifies the time to live for Cisco DP PDUs. Valid values are from 10 to 255 seconds.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set Cisco DP hold time to 180 seconds:

```
C3(su)->set ciscodp hold-time 180
```

set ciscodp port

Use this command to set the status, voice VLAN, extended trust mode, and CoS priority for untrusted traffic for the Cisco Discovery Protocol on one or more ports.

Syntax

set ciscodp port {[**status** {**disable** | **enable**}] [**vvid** {*vlan-id* | **none** | **dot1p** | **untagged**}] [**trusted** {**yes** | **no**}] [**cos** *value*]} *port-string*

Parameters

status	Sets the CiscoDP port operational status.
disable	Does not transmit or process CiscoDP PDUs.
enable	Transmits and processes CiscoDP PDUs.
vvid	Sets the port voice VLAN for CiscoDP PDU transmission.
vlan-id	Specifies the VLAN ID, range 1-4093.
none	No voice VLAN will be used in CiscoDP PDUs. This is the default.
dot1p	Instructs attached phone to send 802.1p tagged frames.
untagged	Instructs attached phone to send untagged frames.
trusted	Sets the extended trust mode on the port.
yes	Instructs attached phone to allow the device connected to it to transmit traffic containing any CoS or Layer 2 802.1p marking. This is the default value.
no	Instructs attached phone to overwrite the 802.1p tag of traffic transmitted by the device connected to it to 0, by default, or to the value configured with the **cos** parameter.
cos *value*	Instructs attached phone to overwrite the 802.1p tag of traffic transmitted by the device connected to it with the specified *value*, when the trust mode of the port is set to untrusted. *Value* can range from 0 to 7, with 0 indicating the lowest priority.
port-string	Specifies the port(s) on which status will be set.

Defaults

- Status: enabled
- Voice VLAN: none
- Trust mode: trusted
- CoS value: 0

Mode

Switch mode, read-write.

Usage

The following points describe how the Cisco DP extended trust settings work on the switch.

- A Cisco DP port trust status of trusted or untrusted is only meaningful when a Cisco IP phone is connected to a switch port and a PC or other device is connected to the back of the Cisco IP phone.
- A Cisco DP port state of trusted or untrusted only affects tagged traffic transmitted by the device connected to the Cisco IP phone. Untagged traffic transmitted by the device connected to the Cisco IP phone is unaffected by this setting.
- If the switch port is configured to a Cisco DP trust state of **trusted** (with the **trusted yes** parameter of this command), this setting is communicated to the Cisco IP phone instructing it to allow the device connected to it to transmit traffic containing any CoS or Layer 2 802.1p marking.

- If the switch port is configured to a Cisco DP trust state of **untrusted** (**trusted no**), this setting is communicated to the Cisco IP phone instructing it to overwrite the 802.1p tag of traffic transmitted by the device connected to it to 0, by default, or to the value specified by the **cos** parameter of this command.
- There is a one-to-one correlation between the value set with the **cos** parameter and the 802.1p value assigned to ingressed traffic by the Cisco IP phone. A value of 0 equates to an 802.1p priority of 0. Therefore, a value of 7 is given the highest priority.

Note: The Cisco Discovery Protocol must be globally enabled using the **set ciscodp status** command before operational status can be set on individual ports.

Examples

This example shows how to set the Cisco DP port voice VLAN ID to 3 on port ge.1.6 and enable the port operational state.

```
C3(rw)->set ciscodp port status enable vvid 3 ge.1.6
```

This example shows how to set the Cisco DP extended trust mode to untrusted on port ge.1.5 and set the CoS priority to 1.

```
C3(rw)->set ciscodp port trusted no cos 1 ge.1.5
```

clear ciscodp

Use this command to clear the Cisco discovery protocol back to the default values.

Syntax

clear ciscodp [**status** | **timer** | **holdtime** | {**port** {**status** | **vvid** | **trust** | **cos**} [*port-string*]}]

Parameters

status	Clears global CiscoDP enable status to default of auto.
timer	Clears the time between CiscoDP PDU transmissions to default of 60 seconds.
holdtime	Clears the time-to-live for CiscoDP PDU data to default of 180 seconds.
port	Clears the CiscoDP port configuration.
status	Clears the individual port operational status to the default of enabled.
vvid	Clears the individual port voice VLAN for CiscoDP PDU transmission to 0.
trust	Clears the trust mode configuration of the port to trusted.
cos	Clears the CoS priority for untrusted traffic of the port to 0.
port-string	(Optional) Specifies the port(s) on which status will be set.

Defaults

If no parameters are entered, all Cisco DP parameters are reset to the defaults globally and for all ports.

Mode

Switch mode, read-write.

Examples

This example shows how to clear all the Cisco DP parameters back to the default settings.

```
C3(rw)->clear ciscodp
```

This example shows how to clear the Cisco DP status on port ge.1.5.

```
C3(rw)->clear ciscodp port status ge.1.5
```

Configuring Link Layer Discovery Protocol and LLDP-MED

Overview

The Link Layer Discovery Protocol (LLPD) provides an industry standard, vendor-neutral way to allow network devices to advertise their identities and capabilities on a local area network, and to discover that information about their neighbors.

LLDP-MED is an enhancement to LLDP that provides the following benefits:

- Auto-discovery of LAN policies, such as VLAN id, 802.1p priority, and DiffServ codepoint settings, leading to “plug-and-play” networking
- Device location and topology discovery, allowing creation of location databases and, in the case of VoIP, provision of E911 services
- Extended and automated power management of Power over Ethernet endpoints
- Inventory management, allowing network administrators to track their network devices and to determine their characteristics, such as manufacturer, software and hardware versions, and serial or asset numbers

The information sent by an LLDP-enabled device is extracted and tabulated by its peers. The communication can be done when information changes or on a periodic basis. The information tabulated is aged to ensure that it is kept up to date. Ports can be configured to send this information, receive this information, or both send and receive.

Either LLDP or LLDP-MED, but not both, can be used on an interface between two devices. A switch port uses LLDP-MED when it detects that an LLDP-MED-capable device is connected to it.

LLDP information is contained within a Link Layer Discovery Protocol Data Unit (LLDPDU) sent in a single 802.3 Ethernet frame. The information fields in LLDPDU are a sequence of short, variable-length, information elements known as TLVs — type, length, and value fields where:

- Type identifies what kind of information is being sent
- Length indicates the length of the information string in octets
- Value is the actual information that needs to be sent

The LLDP standard specifies that certain TLVs are mandatory in transmitted LLDPDUs, while others are optional. You can configure on a port-specific basis which optional LLDP and LLDP-MED TLVs should be sent in LLDPDUs.

Purpose

To review and configure LLPD and LLPD-MED.

Commands

The commands used to review and configure the CDP discovery protocol are listed below.

For information about...	Refer to page...
show lldp	6-15
show lldp port status	6-16
show lldp port trap	6-16
show lldp port tx-tlv	6-17
show lldp port location-info	6-17
show lldp port local-info	6-18
show lldp port remote-info	6-21
show lldp port network-policy	6-22
set lldp tx-interval	6-23
set lldp hold-multiplier	6-24
set lldp trap-interval	6-24
set lldp med-fast-repeat	6-25
set lldp port status	6-26
set lldp port trap	6-26
set lldp port med-trap	6-27
set lldp port location-info	6-27
set lldp port tx-tlv	6-28
set lldp port network-policy	6-30
clear lldp	6-31
clear lldp port status	6-32
clear lldp port trap	6-32
clear lldp port med-trap	6-33
clear lldp port location-info	6-33
clear lldp port network-policy	6-34
clear lldp port tx-tlv	6-35

Configuration Tasks

The commands included in this implementation allow you to perform the following configuration tasks:

Step	Task	Command(s)
1.	Configure global system LLDP parameters	**set lldp tx-interval** **set lldp hold-multiplier** **set lldp trap-interval** **set lldp med-fast-repeat** **clear lldp**
2.	Enable/disable specific ports to: • Transmit and process received LLDPDUs • Send LLDP traps • Send LLDP-MED traps	**set/clear lldp port status** **set/clear lldp port trap** **set/clear lldp port med-trap**
3.	Configure an ECS ELIN value for specific ports	**set/clear lldp port location-info**
4.	Configure Network Policy TLVs for specific ports	**set/clear lldp port network-policy**
5.	Configure which optional TLVs should be sent by specific ports. For example, if you configured an ECS ELIN and/or Network Policy TLVs, you must enable those optional TLVs to be transmitted on the specific ports.	**set/clear lldp tx-tlv**

show lldp

Use this command to display LLDP configuration information.

Syntax

show lldp

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display LLDP configuration information.

```
C3(ro)->show lldp
Message Tx Interval        : 30
Message Tx Hold Multiplier : 4
Notification Tx Interval   : 5
MED Fast Start Count       : 3

Tx-Enabled Ports           : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
Rx-Enabled Ports           : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;

Trap-Enabled Ports         : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
MED Trap-Enabled Ports     : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
```

show lldp port status

Use this command to display the LLDP status of one or more ports. The command lists the ports that are enabled to send and receive LLDP PDUs. Ports are enabled or disabled with the set lldp port status command.

Syntax

show lldp port status [*port-string*]

Parameters

port-string	(Optional) Displays LLDP status for one or a range of ports.

Defaults

If *port-string* is not specified, LLDP status information will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display LLDP port status information for all ports.

```
C3(ro)->show lldp port status

Tx-Enabled Ports      : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12

Rx-Enabled Ports      : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12
```

show lldp port trap

Use this command to display the ports that are enabled to send an LLDP notification when a remote system change has been detected or an LLDP-MED notification when a change in the topology has been sensed. Ports are enabled to send LLDP notifications with the set lldp port trap command and to send LLDP-MED notifications with the set lldp port med-trap command.

Syntax

show lldp port trap [*port-string*]

Parameters

port-string	(Optional) Displays the port or range of ports that have been enabled to send LLDP and/or LLDP-MED notifications.

Defaults

If *port-string* is not specified, LLDP port trap information will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display LLDP port trap information for all ports.

```
C3(ro)->show lldp port trap

Trap-Enabled Ports    :
MED Trap-Enabled Ports:
```

show lldp port tx-tlv

Use this command to display information about which optional TLVs have been configured to be transmitted on ports. Ports are configured to send optional TLVs with the set lldp port tx-tlv command.

Syntax

show lldp port tx-tlv [*port-string*]

Parameters

port-string	(Optional) Displays information about TLV configuration for one or a range of ports.

Defaults

If *port-string* is not specified, TLV configuration information will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display transmit TLV information for three ports.

```
C3(ro)->show lldp port tx-tlv ge.1.1-3

* Means TLV is supported and enabled on this port
o Means TLV is supported on this port
  Means TLV is not supported on this port
Column Pro Id uses letter notation for enable: s-stp, l-lacp, g-gvrp

Ports    Port Sys  Sys  Sys Mgmt Vlan Pro  MAC PoE Link Max   MED MED MED MED
         Desc Name Desc Cap Addr Id   Id   PHY     Aggr Frame Cap Pol Loc PoE
-------  ---- ---- ---- --- ---- ---- ---- --- --- ---- ----  --- --- --- ---
ge.1.1   *    *    *    *   *    *    slg  *       *    *     *       *
ge.1.2   *    *    *    *   *    *    slg  *       *    *
ge.1.3   *    *    *    *   *    *    slg  *       *    *     *      *
```

show lldp port location-info

Use this command to display configured location information for one or more ports. Ports are configured with a location value using the set lldp port location-info command.

Syntax

show lldp port location-info [*port-string*]

Parameters

port-string	(Optional) Displays port location information for one or a range of ports.

Defaults

If *port-string* is not specified, port location configuration information will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display port location information for three ports.

```
C3(ro)->show lldp port location-info ge.1.1-3

Ports      Type            Location
--------   -------------   -------------------------
ge.1.1     ELIN             1234567890
ge.1.2     ELIN             1234567890
ge.1.3     ELIN             1234567890
```

show lldp port local-info

Use this command to display the local system information stored for one or more ports. You can use this information to detect misconfigurations or incompatibilities between the local port and the attached endpoint device (remote port).

Syntax

show lldp port local-info [*port-string*]

Parameters

port-string	(Optional) Displays local system information for one or a range of ports.

Defaults

If *port-string* is not specified, local system information will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display the local system information stored for port ge.4.1. Table 6-4 describes the output fields of this command.

```
C3(rw)->show lldp port local-info ge.4.1

Local Port  : ge.4.1      Local Port Id: ge.4.1
--------------------
Port Desc   : ... 1000BASE-TX RJ45 Gigabit Ethernet Frontpanel Port
```

```
Mgmt Addr   : 10.21.64.100
Chassis ID  : 00-E0-63-93-74-A5
Sys Name    : LLDP PoE test Chassis
Sys Desc    : Enterasys Networks, Inc.
Sys Cap Supported/Enabled     : bridge,router/bridge

Auto-Neg Supported/Enabled    : yes/yes
Auto-Neg Advertised           : 10BASE-T, 10BASE-TFD,
                                100BASE-TX, 100BASE-TXFD,
                                1000BASE-TFD,
                                Bpause
Operational Speed/Duplex/Type : 100 full tx
Max Frame Size (bytes)        : 1522

Vlan Id                       : 1
LAG Supported/Enabled/Id      : no/no/0
Protocol Id : Spanning Tree v-3 (IEEE802.1s)
              LACP v-1
              GVRP

Network Policy
(app/tag/vlanId/cos/dscp)     : voice/tagged/10/3/5
                                voice signaling/tagged/10/3/5
                                guest voice/tagged/10/3/5
                                guest voice signaling/tagged/10/3/5
                                softphone voice/tagged/10/3/5
                                video conferencing/tagged/10/3/5
                                streaming video/tagged/10/3/5
                                video signaling/tagged/10/3/5
ECS ELIN    : 123456789012345678901234

PoE Device                    : PSE device
PoE Power Source              : primary
PoE MDI Supported/Enabled     : yes/yes
PoE Pair Controllable/Used    : false/spare
PoE Power Class               : 2
PoE Power Limit (mW)          : 15400
PoE Power Priority            : high
```

Table 6-4 describes the information displayed by the **show lldp port local-info** command.

Table 6-4 show lldp port local-info Output Details

Output Field	What it Displays...
Local Port	Identifies the port for which local system information is displayed.
Local Port Id	Mandatory basic LLDP TLV that identifies the port transmitting the LLDPDU. Value is ifName object defined in RFC 2863.
Port Desc	Optional basic LLDP TLV. Value is ifDescr object defined in RFC 2863.
Mgmt Addr	Optional basic LLDP TLV. IPv4 address of host interface.
Chassis ID	Mandatory basic LLDP TLV that identifies the chassis transmitting the LLDPDU. Value is MAC address of chassis.
Sys Name	Optional basic LLDP TLV. Value is the administratively assigned name for the system.
Sys Desc	Optional basic LLDP TLV. Value is sysDescr object defined in RFC 3418.
Sys Cap Supported/Enabled	Optional basic LLDP TLV. System capabilities, value can be bridge and/or router.

Table 6-4 show lldp port local-info Output Details (Continued)

Output Field	What it Displays...
Auto-Neg Supported/Enabled	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Auto-negotiation supported and enabled settings should be the same on the two systems attached to the same link.
Auto-Neg Advertised	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Lists the configured advertised values on the port.
Operational Speed/Duplex/ Type	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Lists the operational MAU type, duplex, and speed of the port. If the received TLV indicates that auto-negotiation is supported but not enabled, these values will be used by the port.
Max Frame Size (bytes)	IEEE 802.3 Extensions Maximum Frame Size TLV. Value indicates maximum frame size capability of the device's MAC and PHY. In normal mode, max frame size is 1522 bytes. In jumbo mode, max frame size is 10239 bytes.
Vlan Id	IEEE 802.1 Extensions Port VLAN ID TLV. Value is port VLAN ID (pvid).
LAG Supported/Enabled/Id	IEEE 802.3 Extensions Link Aggregation TLV. Values indicate whether the link associated with this port can be aggregated, whether it is currently aggregated, and if aggregated, the aggregated port identifier.
Protocol Id	IEEE 802.1 Extensions Protocol Identity TLV. Values can include Spanning tree, LACP, and GARP protocols and versions. Only those protocols enabled on the port are displayed.
Network Policy (app/tag/vlanId/cos/dscp)	LLDP-MED Extensions Network Policy TLV. For all applications enabled on the port to be transmitted in a TLV, displays the application name, VLAN type (tagged or untagged), VLAN Id, and both the Layer 2 and Layer 3 priorities associated with the application.
ECS ELIN	LLDP-MED Extensions Location Identification TLV. Emergency Call Services (ECS) Emergency Location Identification Number (ELIN) is currently the only type supported. Value is the ELIN configured on this port.
PoE Device	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Value is the Power Type of the device. On a switch port, the value is Power Sourcing Entity (PSE).
PoE Power Source	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Value can be primary or backup, indicating whether the PSE is using its primary or backup power source.
PoE MDI Supported/Enabled	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates whether sending the Power via MDI TLV is supported/enabled. Value can be yes or no.
PoE Pair Controllable/Used	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates whether pair selection can be controlled on the given port (refer to RFC 3621). Value for Controllable can be true or false. Value of Used can be signal (signal pairs only are in use) or spare (spare pairs only are in use).
PoE Power Class	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the power class supplied by the port. Value can range from 0 to 4.

Table 6-4 show lldp port local-info Output Details (Continued)

Output Field	What it Displays...
PoE Power Limit (mW)	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the total power the port is capable of sourcing over a maximum length cable, based on its current configuration, in milli-Watts.
PoE Power Priority	LLDP-MED Extensions Extended Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the power priority configured on the port. Value can be critical, high, or low.

show lldp port remote-info

Use this command to display the remote system information stored for a remote device connected to a local port. You can use this information to detect misconfigurations or incompatibilities between the local port and the attached endpoint device (remote port).

Syntax

show lldp port remote-info [*port-string*]

Parameters

port-string	(Optional) Displays remote system information for one or a range of ports.

Defaults

If *port-string* is not specified, remote system information will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display the remote system information stored for port ge.3.1. The remote system information was received from an IP phone, which is an LLDP-MED-enabled device. Table 6-5 describes the output fields that are unique to the remote system information displayed for a MED-enabled device.

```
C3(ro)->show lldp port remote-info ge.3.1
Local Port  : ge.3.1     Remote Port Id : 00-09-6e-0e-14-3d
---------------------
Mgmt Addr   : 0.0.0.0
Chassis ID  : 0.0.0.0
Device Type : Communication Device Endpoint (class III)
Sys Name    : AVE0E143D
Sys Cap Supported/Enabled     : bridge,telephone/bridge

Auto-Neg Supported/Enabled    : yes/yes
Auto-Neg Advertised           : 10BASE-T, 10BASE-TFD
                              : 100BASE-TX, 100BASE-TXFD
                              : pause, Spause
Operational Speed/Duplex/Type : 100/full/TX
Network Policy
(app/tag/vlanId/cos/dscp)     : voice/untagged/0/6/46
```

```
Hardware Revision            : 4610D01A
Firmware Revision            : b10d01b2_7.bin
Software Revision            : a10d01b2_7.bin
Serial Number                : 05GM42004348
Manufacturer                 : Avaya
Model Number                 : 4610
```

Note that the information fields displayed by the **show lldp port remote-info** command will vary, depending on the type of remote device that is connected to the port.

Table 6-5 describes the output fields that are unique to the remote system information database. Refer to Table 6-4 on page 19 for descriptions of the information fields that are common to both the local and the remote system information databases.

Table 6-5 show lldp port remote-info Output Display

Output Field	What it Displays...
Remote Port Id	Displays whatever port Id information received in the LLDPDU from the remote device. In this case, the port Id is MAC address of remote device.
Device Type	Mandatory LLDP-MED Capabilities TLV. Displayed only when the port is connected to an LLDP-MED-capable endpoint device.
Hardware Revision	LLDP-MED Extensions Inventory Management TLV component.
Firmware Revision	LLDP-MED Extensions Inventory Management TLV component.
Software Revision	LLDP-MED Extensions Inventory Management TLV component.
Serial Number	LLDP-MED Extensions Inventory Management TLV component.
Manufacturer	LLDP-MED Extensions Inventory Management TLV component.
Model Number	LLDP-MED Extensions Inventory Management TLV component.
Asset ID	LLDP-MED Extensions Inventory Management TLV component. In the above example, no asset ID was received from the remote device so the field is not displayed.

show lldp port network-policy

Use this command to display LLDP port network policy configuration information. Network policy information is configured using the set lldp port network-policy command.

Syntax

show lldp port network-policy {**all** | **voice** | **voice-signaling** | **guest-voice** | **guest-voice-signaling** | **softphone-voice** | **video-conferencing** | **streaming-video** | **video-signaling**} [*port-string*]

Parameters

all	Displays information about all network policy applications.
voice	Displays information about only the voice application type.
voice-signaling	Displays information about only the voice signaling application type.
guest-voice	Displays information about only the guest voice application type.
guest-voice-signaling	Displays information about only the guest voice signaling application type.

softphone-voice	Displays information about only the softphone voice application type.
video-conferencing	Displays information about only the video conferencing application type.
streaming-video	Displays information about only the streaming video application type.
video-signaling	Displays information about only the video signaling application type.
port-string	(Optional) Displays information about LLDP network policy for one or a range of ports.

Defaults

If *port-string* is not specified, only non-default values will be displayed for all ports that have non-default values configured.

If a *port-string* is specified, then all values, default and non-default, are displayed for the specified ports.

Mode

Switch command, read-only.

Example

This example shows how to display all LLDP network policy information for ge.1.1.

```
C3(ro)->show lldp port network-policy all ge.1.1

Ports    Application            State     Tag       Vlan-Id   Cos   Dscp
-------  ---------------------  --------  --------  -------   ---   ---
ge.1.1   voice                  enabled   untagged  1         0     0
         voice signaling        enabled   untagged  1         0     0
         guest voice            enabled   untagged  1         0     0
         guest voice signaling  enabled   untagged  1         0     0
         softphone voice        enabled   untagged  1         0     0
         video conferencing     enabled   untagged  1         0     0
         streaming video        enabled   untagged  1         0     0
         video signaling        enabled   untagged  1         0     0
```

set lldp tx-interval

Use this command to set the time, in seconds, between successive LLDP frame transmissions initiated by changes in the LLDP local system information.

Syntax

`set lldp tx-interval` *`frequency`*

Parameters

frequency	Specifies the number of seconds between transmissions of LLDP frames. Value can range from 5 to 32,768 seconds. The default is 30 seconds.

Defaults

None.

Mode

Switch command, read-write.

Example

This example sets the transmit interval to 20 seconds.

```
C3(rw)->set lldp tx-interval 20
```

set lldp hold-multiplier

Use this command to set the time-to-live value used in LLDP frames sent by this device. The time-to-live for LLDPDU data is calculated by multiplying the transmit interval by the hold multiplier value.

Syntax

set lldp hold-multiplier *multiplier-val*

Parameters

multiplier-val	Specifies the multiplier to apply to the transmit interval to determine the time-to-live value. Value can range from 2 to 10. Default value is 4.

Defaults

None.

Mode

Switch command, read-write.

Example

This example sets the transmit interval to 20 seconds and the hold multiplier to 5, which will configure a time-to-live of 100 to be used in the TTL field in the LLDPDU header.

```
C3(rw)->set lldp tx-interval 20
C3(rw)->set lldp hold-multiplier 5
```

set lldp trap-interval

Use this command to set the minimum interval between LLDP notifications sent by this device. LLDP notifications are sent when a remote system change has been detected.

Syntax

set lldp trap-interval *frequency*

Parameters

frequency	Specifies the minimum time between LLDP trap transmissions, in seconds. The value can range from 5 to 3600 seconds. The default value is 5 seconds.

Defaults

None.

Mode

Switch command, read-write.

Example

This example sets the minimum interval between LLDP traps to 10 seconds.

```
C3(rw)->set lldp trap-interval 10
```

set lldp med-fast-repeat

Network connectivity devices transmit only LLDP TLVs in LLDPDUs until they detect that an LLDP-MED endpoint device has connected to a port. At that point, the network connectivity device starts sending LLDP-MED TLVs at a fast start rate on that port. Use this command to set the number of successive LLDPDUs (with LLDP-MED TLVs) to be sent for one complete fast start interval.

Syntax

`set lldp med-fast-repeat` *`count`*

Parameters

count	Specifies the number of fast start LLDPDUs to be sent when an LLDP-MED endpoint device is detected. Value can range from 1 to 10. Default is 3.

Defaults

None.

Mode

Switch command, read-write.

Example

This example sets the number of fast start LLDPDUs to be sent to 4.

```
C3(rw)->set lldp med-fast-repeat 4
```

set lldp port status

Use this command to enable or disable transmitting and processing received LLDPDUs on a port or range of ports.

Syntax

set lldp port status {**tx-enable** | **rx-enable** | **both** | **disable**} *port-string*

Parameters

tx-enable	Enables transmitting LLDPDUs on the specified ports.
rx-enable	Enables receiving and processing LLDPDUs from remote systems on the specified ports.
both	Enables both transmitting and processing received LLDPDUs on the specified ports.
disable	Disables both transmitting and processing received LLDPDUs on the specified ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, read-write.

Example

This example enables both transmitting LLDPDUs and receiving and processing LLDPDUs from remote systems on ports ge.1.1 through ge.1.6.

```
C3(rw)->set lldp port status both ge.1.1-6
```

set lldp port trap

Use this command to enable or disable sending LLDP notifications (traps) when a remote system change is detected.

Syntax

set lldp port trap {**enable** | **disable**} *port-string*

Parameters

enable	Enable transmitting LLDP traps on the specified ports.
disable	Disable transmitting LLDP traps on the specified ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, read-write.

Example

This example enables transmitting LLDP traps on ports ge.1.1 through ge.1.6.

```
C3(rw)->set lldp port trap enable ge.1.1-6
```

set lldp port med-trap

Use this command to enable or disable sending an LLDP-MED notification when a change in the topology has been sensed on the port (that is, a remote endpoint device has been attached or removed from the port).

Syntax

set lldp port med-trap {**enable** | **disable**} *port-string*

Parameters

enable	Enables transmitting LLDP-MED traps on the specified ports.
disable	Disables transmitting LLDP-MED traps on the specified ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, read-write.

Example

This example enables transmitting LLDP-MED traps on ports ge.1.1 through ge.1.6.

```
C3(rw)->set lldp port med-trap enable ge.1.1-6
```

set lldp port location-info

Use this command to configure LLDP-MED location information on a port or range of ports. Currently, only Emergency Call Services (ECS) Emergency Location Identification Number (ELIN) is supported.

Syntax

set lldp port location-info elin *elin-string port-string*

Parameters

elin	Specifies that the ECS ELIN data format is to be used.
elin-string	Specifies the location identifier. Value can be from 10 to 25 numerical characters.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, read-write.

Example

After you configure a location information value, you must also configure the port to send the Location Information TLV with the set lldp port tx-tlv command. This example configures the ELIN identifier 5551234567 on ports ge.1.1 through ge.1.6 and then configures the ports to send the Location Information TLV.

```
C3(rw)->set lldp port location-info 5551234567 ge.1.1-6
C3(rw)->set lldp port tx-tlv med-loc ge.1.1-6
```

set lldp port tx-tlv

Use this command to select the optional LLDP and LLDP-MED TLVs to be transmitted in LLDPDUs by the specified port or ports. Use the show lldp port local-info command to display the values of these TLVs for the port.

Syntax

`set lldp port tx-tlv` {[**`all`**] | [**`port-desc`**] [**`sys-name`**] [**`sys-desc`**] [**`sys-cap`**] [**`mgmt-addr`**] [**`vlan-id`**] [**`stp`**] [**`lacp`**] [**`gvrp`**] [**`mac-phy`**] [**`poe`**] [**`link-aggr`**] [**`max-frame`**] [**`med-cap`**] [**`med-pol`**] [**`med-loc`**] [**`med-poe`**]} *`port-string`*

Parameters

all	Adds all optional TLVs to transmitted LLDPDUs.
port-desc	Port Description optional basic LLDP TLV. Value sent is ifDescr object defined in RFC 2863.
sys-name	System Name optional basic LLDP TLV. Value sent is the administratively assigned name for the system.
sys-desc	System Description optional basic LLDP TLV. Value sent is sysDescr object defined in RFC 3418.
sys-cap	System Capabilities optional basic LLDP TLV. For a network connectivity device, value sent can be bridge and/or router.
mgmt-addr	Management Address optional basic LLDP TLV. Value sent is IPv4 address of host interface.
vlan-id	Port VLAN ID IEEE 802.1 Extensions TLV. Value sent is port VLAN ID (PVID).
stp	Spanning Tree information defined by Protocol Identity IEEE 802.1 Extensions TLV. If STP is enabled on the port, value sent includes version of protocol being used.
lacp	LACP information defined by Protocol Identity IEEE 802.1 Extensions TLV. If LACP is enabled on the port, value sent includes version of protocol being used.

gvrp	GVRP information defined by Protocol Identity IEEE 802.1 Extensions TLV. If LACP is enabled on the port, value sent includes version of protocol being used.
mac-phy	MAC-PHY Configuration/Status IEEE 802.3 Extensions TLV. Value sent includes the operational MAU type, duplex, and speed of the port.
poe	Power via MDI IEEE 802.3 Extensions TLV. Values sent include whether pair selection can be controlled on port, and the power class supplied by the port. Only valid for PoE-enabled ports.
link-aggr	Link Aggregation IEEE 802.3 Extensions TLV. Values sent indicate whether the link associated with this port can be aggregated, whether it is currently aggregated, and if aggregated, the aggregated port identifier.
max-frame	Maximum Frame Size IEEE 802.3 Extensions TLV. Value sent indicates maximum frame size of the port's MAC and PHY.
med-cap	LLDP-MED Capabilities TLV.Value sent indicates the capabilities (whether the device supports location information, network policy, extended power via MDI) and Device Type (network connectivity device) of the sending device.
med-pol	LLDP-MED Network Policy TLV. Values sent include application name, VLAN type (tagged or untagged), VLAN ID, and both Layer 2 and Layer 3 priorities associated with application, for all applications enabled on the port. See the set lldp port network-policy command for more information.
med-loc	LLDP-MED Location Identification TLV. Value sent is the ECS ELIN value configured on the port. See the set lldp port location-info command for more information.
med-poe	LLDP-MED Extended Power via MDI TLV. Values sent include the Power Limit (total power the port is capable of sourcing over a maximum length cable) and the power priority configured on the port. Only valid for PoE-enabled ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, read-write.

Example

This example configures the management address, MED capability, MED network policy, and MED location identification TLVs to be sent in LLDPDUs by port `ge.1.1`.

```
C3(rw)->set lldp port tx-tlv mgmt-addr med-cap med-pol med-loc ge.1.1
```

set lldp port network-policy

Use this command to configure LLDP network policies for a set of applications on a port or range of ports. The policies configured with this command are sent in LLDPDUs as LLDP-MED Network Policy TLVs. Multiple Network Policy TLVs can be sent in a single LLDPDU.

Syntax

```
set lldp port network-policy {all | voice | voice-signaling | guest-voice |
guest-voice-signaling | softphone-voice | video-conferencing | streaming-video |
video-signaling} [state {enable | disable}] [tag {tagged | untagged}]
[vid {vlan-id | dot1p}] [cos cos-value] [dscp dscp-value] port-string
```

Parameters

all	Configures all applications.
voice	Configures the voice application.
voice-signaling	Configures the voice signaling application. This application will not be advertised if the **voice** application is configured with the same parameters.
guest-voice	Configures the guest voice application.
guest-voice-signaling	Configures the guest voice signaling application. This application will not be advertised if the **guest-voice** application is configured with the same parameters.
softphone-voice	Configures the softphone voice application.
video-conferencing	Configures the video conferencing application.
streaming-video	Configures the streaming video application.
video-signaling	Configures the video signaling application. This application will not be advertised if the **video-conferencing** application is configured with the same parameters.
state enable | **disable**	(Optional) Enables or disables advertising the application information being configured.
tag tagged | **untagged**	(Optional) Indicates whether the application being configured is using a tagged or untagged VLAN. If untagged, both the VLAN ID and the CoS priority fields are ignored and only the DSCP value has relevance.
vid *vlan-id* | **dot1p**	(Optional) VLAN identifier for the port. The value of *vlan-id* can range from 1 to 4093. Use **dot1p** if the device is using priority tagged frames, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used.
cos *cos-value*	(Optional) Specifies the Layer 2 priority to be used for the application being configured. The value can range from 0 to 7. A value of 0 represents use of the default priority as defined in IEEE 802.1D.
dscp *dscp-value*	(Optional) Specifies the DSCP value to be used to provide Diffserv node behavior for the application being configured. The value can range from 0 to 63. A value of 0 represents use of the default DSCP value as defined in RFC 2475.

port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, read-write.

Usage

This feature allows administrators to quickly provision LLDP end-points via the switch. LLDP clients will use these LLDP network policy parameters for traffic originating from the end-point.

As described in the ANSI/TIA Standards document 1057, the Network Policy TLV is "intended for use with applications that have specific real-time network policy requirements, such as interactive voice and/or video services" and should be implemented only on direct links between network connectivity devices and endpoint devices. Refer to the ANSI/TIA Standards document 1057 for descriptions of the application types.

After you configure Network Policy TLVs, you must also configure the port to send the Network Policy TLV with the set lldp port tx-tlv command.

Example

This example configures the voice application TLV on port ge.2.1 and then configures the port to send the Network Policy TLV.

```
C3(rw)->set lldp port network-policy voice state enable tag tagged vlan dot1p
ge.2.1
C3(rw)->set lldp port tx-tlv med-pol ge.2.1
```

clear lldp

Use this command to return LLDP parameters to their default values.

Syntax

clear lldp {**all** | **tx-interval** | **hold-multiplier** | **trap-interval** | **med-fast-repeat**}

Parameters

all	Returns **all** LLDP configuration parameters to their default values, including port LLDP configuration parameters.
tx-interval	Returns the number of seconds between transmissions of LLDP frames.to the default of 30 seconds.
hold-multiplier	Returns the multiplier to apply to the transmit interval to determine the time-to-live value to the default value of 4.
trap-interval	Returns the minimum time between LLSP trap transmissions to the default value of 5 seconds.
med-fast-repeat	Returns the number of fast start LLDPDUs to be sent when an LLDP-MED endpoint device is detected to the default of 3.

Defaults

None.

Mode

Switch command, read-write.

Example

This example returns the transmit interval to the default value of 30 seconds.

```
C3(rw)->clear lldp tx-interval
```

clear lldp port status

Use this command to return the port status to the default value of both (both transmitting and processing received LLDPDUs are enabled).

Syntax

clear lldp port status *port-string*

Parameters

port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, read-write.

Example

This example returns port `ge.1.1` to the default state of enabled for both transmitting and processing received LLDPDUs.

```
C3(rw)->clear lldp port status ge.1.1
```

clear lldp port trap

Use this command to return the port LLDP trap setting to the default value of disabled.

Syntax

clear lldp port trap *port-string*

Parameters

port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, read-write.

Example

This example returns port `ge.1.1` to the default LLDP trap state of disabled.

```
C3(rw)->clear lldp port trap ge.1.1
```

clear lldp port med-trap

Use this command to return the port LLDP-MED trap setting to the default value of disabled.

Syntax

`clear lldp port med-trap` *`port-string`*

Parameters

port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, read-write.

Example

This example returns port `ge.1.1` to the default LLDP-MED trap state of disabled.

```
C3(rw)->clear lldp port med-trap ge.1.1
```

clear lldp port location-info

Use this command to return the port ECS ELIN location setting to the default value of null.

Syntax

`clear lldp port location-info elin` *`port-string`*

Parameters

elin	Specifies that the ECS ELIN location information value should be cleared.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, read-write.

Example

This example returns the location information ELIN value on port ge.1.1 to the default value of null.

```
C3(rw)->clear lldp port location-info elin ge.1.1
```

clear lldp port network-policy

Use this command to return LLDP network policy for a set of applications on a port or range of ports to default values.

Syntax

clear lldp port network-policy {**all** | **voice** | **voice-signaling** | **guest-voice** | **guest-voice-signaling** | **softphone-voice** | **video-conferencing** | **streaming-video** | **video-signaling**} {[**state**] [**tag**] [**vid**] [**cos**] [**dscp**]} *port-string*

Parameters

all	Applies command to all applications.
voice	Applies command to the voice application.
voice-signaling	Applies command to the voice signaling application.
guest-voice	Applies command to the guest voice application.
guest-voice-signaling	Applies command to the guest voice signaling application.
softphone-voice	Applies command to the softphone voice application.
video-conferencing	Applies command to the video conferencing application.
streaming-video	Applies command to the streaming video application.
video-signaling	Applies command to the video signaling application.
state	(Optional) Clears the state of advertising the application information being configured to disabled.
tag	(Optional) Clears the tag value of the application being configured to untagged.
vid	(Optional) Clears the VLAN identifier for the port to the default value of 1.
cos	(Optional) Clears the Layer 2 priority to be used for the application being configured to the default value of 0. (A value of 0 represents use of the default priority as defined in IEEE 802.1D.)
dscp	(Optional) Clears the DSCP value to be used to provide Diffserv node behavior for the application being configured to the default value of 0. (A value of 0 represents use of the default DSCP value as defined in RFC 2475.)
port-string	Specifies the port or range of ports to be affected.

Defaults

At least one application (or **all**) and one policy parameter must be specified.

Mode

Switch command, read-write.

Example

This example returns all network policy values for all applications on port ge.1.1 to their default values.

```
C3(rw)->clear lldp port network-policy all state tag vid cos dscp ge.1.1
```

clear lldp port tx-tlv

Use this command to clear the optional LLDP and LLDP-MED TLVs to be transmitted in LLDPDUs by the specified port or ports to the default value of disabled.

Syntax

clear lldp port tx-tlv {[**all**] | [**port-desc**] [**sys-name**] [**sys-desc**] [**sys-cap**] [**mgmt-addr**] [**vlan-id**] [**stp**] [**lacp**] [**gvrp**] [**mac-phy**] [**poe**] [**link-aggr**] [**max-frame**] [**med-cap**] [**med-pol**] [**med-loc**] [**med-poe**]} *port-string*

Parameters

all	Disables all optional TLVs from being transmitted in LLDPDUs.
port-desc	Disables the Port Description optional basic LLDP TLV from being transmitted in LLDPDUs.
sys-name	Disables the System Name optional basic LLDP TLV from being transmitted in LLDPDUs.
sys-desc	Disables the System Description optional basic LLDP TLV from being transmitted in LLDPDUs.
sys-cap	Disables the System Capabilities optional basic LLDP TLV from being transmitted in LLDPDUs.
mgmt-addr	Disables the Management Address optional basic LLDP TLV from being transmitted in LLDPDUs.
vlan-id	Disables the Port VLAN ID IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
stp	Disables the Spanning Tree information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
lacp	Disables the LACP information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
gvrp	Disables the GVRP information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
mac-phy	Disables the MAC-PHY Configuration/Status IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
poe	Disables the Power via MDI IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs. Only valid for PoE-enabled ports.
link-aggr	Disables the Link Aggregation IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
max-frame	Disables the Maximum Frame Size IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
med-cap	Disables the LLDP-MED Capabilities TLV from being transmitted in LLDPDUs.

med-pol	Disables the LLDP-MED Network Policy TLV from being transmitted in LLDPDUs.
med-loc	Disables the LLDP-MED Location Identification TLV from being transmitted in LLDPDUs.
med-poe	Disables the LLDP-MED Extended Power via MDI TLV from being transmitted in LLDPDUs. Only valid for PoE-enabled ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

Switch command, read-write.

Example

This example disables the management address, MED capability, MED network policy, and MED location identification TLVs from being sent in LLDPDUs by port `ge.1.1`.

```
C3(rw)->clear lldp port tx-tlv mgmt-addr med-cap med-pol med-loc ge.1.1
```

7

Port Configuration

This chapter describes the Port Configuration set of commands and how to use them.

Port Configuration Summary

Port String Syntax Used in the CLI

Commands requiring a *port-string* parameter use the following syntax to designate port type, slot location, and port number:

port type.unit_or_slot number.port number

Where **port type** can be:
fe for 100-Mbps Ethernet
ge for 1-Gbps Ethernet
tg for 10-Gbps Ethernet
host for the host port
vlan for vlan interfaces
lag for IEEE802.3 link aggregation ports

Where unit_or_slotnumber can be:
1 - **8** for switch units in a stack

Where **port number** depends on the device. The highest valid port number is dependent on the number of ports in the device and the port type.

Port Slot/Unit Parameters Used in the CLI

The "unit" parameter is often used interchangeably with "module" in the standalone switch CLI to indicate a module slot location.

Examples

Note: You can use a wildcard (*) to indicate all of an item. For example, fe.3.* would represent all 100Mbps Ethernet (fe) ports in slot 3, and ge.3 * would represent all 1-Gigabit Ethernet (ge) ports in slot 3.

This example shows the *port-string* syntax for specifying the 1-Gigabit Ethernet port 14 in slot unit 3.

```
ge.3.14
```

This example shows the *port-string* syntax for specifying all 1-Gigabit Ethernet ports in slot unit 3 in the system.

```
ge.3.*
```

This example shows the *port-string* syntax for specifying all ports (of any interface type) in the system.

```
*.*.*
```

Reviewing Port Status

Purpose

To display operating status, duplex mode, speed, port type, and statistical information about traffic received and transmitted through one or all switch ports on the device.

Commands

For information about...	Refer to page...
show port	7-3
show port status	7-3
show port counters	7-4
clear port counters	7-6
show port cablestatus	7-6

show port

Use this command to display whether or not one or more ports are enabled for switching.

Syntax

show port [*port-string*]

Parameters

port-string	(Optional) Displays operational status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, operational status information for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display operational status information for ge.3.14:

```
C3(su)->show port ge.3.14
Port ge.3.14 enabled
```

show port status

Use this command to display operating and admin status, speed, duplex mode and port type for one or more ports on the device.

Syntax

show port status [*port-string*]

Parameters

port-string	(Optional) Displays status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, status information for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display status information for ge.3.14:

```
C3(su)->show port status ge.3.14

Port          Alias          Oper      Admin    Speed     Duplex   Type
```

```
             (truncated)      Status   Status
------------  -------------  -------  -------  --------  -------  -------------
ge.3.14                      up       up        N/A      N/A      BaseT RJ45
```

Table 7-1 provides an explanation of the command output.

Table 7-1 show port status Output Details

Output Field	What It Displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
Alias (truncated)	Alias configured for the port. For details on using the **set port alias** command, refer to "set port alias" on page 7-9.
Oper Status	Operating status (up or down).
Admin Status	Whether the specified port is enabled (up) or disabled (down). For details on using the **set port disable** command to change the default port status of enabled, refer to "set port disable" on page 7-8. For details on using the **set port enable** command to re-enable ports, refer to "set port enable" on page 7-8.
Speed	Operational speed in Mbps or Kbps of the specified port. For details on using the **set port speed** command to change defaults, refer to "set port speed" on page 7-12.
Duplex	Duplex mode (half or full) of the specified port. For details on using the **set port duplex** command to change defaults, refer to "Setting Auto-Negotiation and Advertised Ability" on page 7-16.
Type	Physical port and interface type.

show port counters

Use this command to display port counter statistics detailing traffic through the device and through all MIB2 network devices.

Syntax

show port counters [*port-string*] [**switch** | **mib2**]

Parameters

port-string	(Optional) Displays counter statistics for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
switch | **mib2**	(Optional) Displays switch or MIB2 statistics. Switch statistics detail performance of the SecureStack C3 device. MIB2 interface statistics detail performance of all network devices.

Defaults

If *port-string* is not specified, counter statistics will be displayed for all ports.

If **mib2** or **switch** are not specified, all counter statistics will be displayed for the specified port(s).

Mode

Switch command, read-only.

Examples

This example shows how to display all counter statistics, including MIB2 network traffic and traffic through the device for ge.3.1:

```
C3(su)->show port counters ge.3.1

Port: ge.3.1   MIB2 Interface: 1
No counter discontinuity time
-------------------------------------------------------------------

MIB2 Interface Counters
-----------------------
In Octets                          0
In Unicast Pkts                    0
In Multicast Pkts                  0
In Broadcast Pkts                  0
In Discards                        0
In Errors                          0
Out Octets                         0
Out Unicasts Pkts                  0
Out Multicast Pkts                 0
Out Broadcast Pkts                 0
Out Errors                         0

802.1Q Switch Counters
----------------------
Frames Received                    0
Frames Transmitted                 0
```

This example shows how to display all ge.3.1 port counter statistics related to traffic through the device.

```
C3(su)->show port counters ge.3.1 switch

Port: ge.3.1          Bridge Port: 2

802.1Q Switch Counters
----------------------
Frames Received                  0
Frames Transmitted               0
```

Table 7-2 provides an explanation of the command output.

Table 7-2 show port counters Output Details

Output Field	What It Displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
MIB2 Interface	MIB2 interface designation.
Bridge Port	IEEE 802.1D bridge port designation.
MIB2 Interface Counters	MIB2 network traffic counts
802.1Q Switch Counters	Counts of frames received, transmitted, and filtered.

clear port counters

Use this command to clear port counter statistics for a port or range of ports.

Syntax

clear port counters [*port-string*]

Parameters

port-string	(Optional) Specifies the port or range of ports to clear port counter statistics.

Defaults

If no *port-string* is specified, port counters are cleared for all ports.

Mode

Switch command, read-write

Example

This example clears the port counters for ge.3.1.

```
C3(rw)->clear port counters ge3.1
```

show port cablestatus

Use this command to troubleshoot and locate faults in copper cable connections on a per port basis. This command is only available on switch platforms that provide 1 Gigabit Ethernet RJ45 ports.

Syntax

show port cablestatus [*port-string*]

Parameters

port-string	(Optional) Specifies the port or ports to show status for.

Defaults

If no port is specified, information about all ports will be displayed.

Mode

Switch command, read-only.

Usage

For 1 Gigabit Ethernet RJ45 ports only, this command will display the status of the port's cable connection (described in Table 7-3 below), and the approximate length of the cable attached to the port. If your switch platform does not support 1 GE RJ45 ports, this command will not be available.

If no cable is attached to the port, the status will be "Open" and no length will be shown. If the port is not a 1GE RJ45 port, the command will return a status of "Not Supported."

Since running the cable diagnostics may momentarily interrupt packet flow, a warning message is displayed and you are prompted to continue.

Example

This example shows the cable status for 1 GE port ge.1.31.

```
C3(su)->show port cablestatus ge.1.31
Warning: port(s) will be offline momentarily.
Do you want to continue (y/n) [n]?y

Port      Status      Length
--------- ---------   -------
ge.1.31   Normal      3(m)-5(m)
```

Table 7-3 provides an explanation of the command output.

Table 7-3 show port cablestatus Output Details

Output Field	What it displays...
Port	Lists the port designation.
Status	Indicates the status of the port. The value is one of the following: **Normal** = normal **Open** = no cable attached to port **Short** = detection of an inter-pair short **Fail** = unknown error or crosstalk **Detach** = indicates ports on stack units that are no longer present, but were previously connected **Not Supported** = ports other than 1GE RJ45 ports
Length	Indicates the approximate length of the cable attached to the port.

Disabling / Enabling and Naming Ports

Purpose

To disable and re-enable one or more ports, and to assign an alias to a port. By default, all ports are enabled at device startup. You may want to disable ports for security or to troubleshoot network issues. Ports may also be assigned an alias for convenience.

Commands

For information about...	Refer to page...
set port disable	7-8
set port enable	7-8
show port alias	7-9
set port alias	7-9

set port disable

Use this command to administratively disable one or more ports. When this command is executed, in addition to disabling the physical Ethernet link, the port will no longer learn entries in the forwarding database.

Syntax

set port disable *port-string*

Parameters

port-string	Specifies the port(s) to disable. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to disable ge.1.1:

```
C3(su)->set port disable ge.1.1
```

set port enable

Use this command to administratively enable one or more ports.

Syntax

set port enable *port-string*

Parameters

port-string	Specifies the port(s) to enable. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to enable ge.1.3:

```
C3(su)->set port enable ge.1.3
```

show port alias

Use this command to display the alias name for one or more ports.

Syntax

show port alias [*port-string*]

Parameters

port-string	(Optional) Displays alias name(s) for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If port-string is not specified, aliases for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display alias information for ports 1-3 on slot 3:

```
C3(rw)->show port alias ge.3.1-3
Port  ge.3.1 user
Port  ge.3.2 user
Port  ge.3.3 Admin
```

set port alias

Use this command to assign an alias name to a port.

Syntax

set port alias *port-string* [*name*]

Parameters

port-string	Specifies the port to which an alias will be assigned. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
name	(Optional) Assigns an alias name to the port. If the alias name contains spaces, the text string must be surrounded by double quotes. Maximum length is 60 characters.

Defaults

If *name* is not specified, the alias assigned to the port will be cleared.

Mode

Switch command, read-write.

Examples

This example shows how to assign the alias “Admin” to ge.3.3:

```
C3(rw)->set port alias ge.3.3 Admin
```

This example shows how to clear the alias for ge.3.3:

```
C3(rw)->set port alias ge.3.3
```

Setting Speed and Duplex Mode

Purpose

To review and set the operational speed in Mbps and the default duplex mode: **Half**, for half duplex, or **Full**, for full duplex for one or more ports.

Note: These settings only take effect on ports that have auto-negotiation disabled.

Commands

For information about...	Refer to page...
show port speed	7-11
set port speed	7-12
show port duplex	7-12
set port duplex	7-16

show port speed

Use this command to display the default speed setting on one or more ports.

Syntax

show port speed [*port-string*]

Parameters

port-string	(Optional) Displays default speed setting(s) for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, default speed settings for all ports will display.

Mode

Switch command, read-only.

Example

This example shows how to display the default speed setting for 1-Gigabit Ethernet port 14 in slot 3:

```
C3(su)->show port speed ge.3.14
default speed is 10 on port ge.3.14.
```

set port speed

Use this command to set the default speed of one or more ports. This setting only takes effect on ports that have auto-negotiation disabled.

Syntax

set port speed *port-string* {**10** | **100** | **1000**}

Parameters

port-string	Specifies the port(s) for which to a speed value will be set. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
10 | **100** | **1000**	Specifies the port speed. Valid values are: **10** Mbps, **100** Mbps, or **1000** Mbps.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set ge.3.3 to a port speed of 10 Mbps:

```
C3(su)->set port speed ge.3.3 10
```

show port duplex

Use this command to display the default duplex setting (half or full) for one or more ports.

Syntax

show port duplex [*port-string*]

Parameters

port-string	(Optional) Displays default duplex setting(s) for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, default duplex settings for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display the default duplex setting for Ethernet port 14 in slot 3:

```
C3(su)->show port duplex ge.3.14
default duplex mode is full on port ge.3.14.
```

set port duplex

Use this command to set the default duplex type for one or more ports. This command will only take effect on ports that have auto-negotiation disabled.

Syntax

set port duplex *port-string* {**full** | **half**}

Parameters

port-string	Specifies the port(s) for which duplex type will be set. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
full | **half**	Sets the port(s) to full-duplex or half-duplex operation.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set ge.1.17 to full duplex:

```
C3(su)->set port duplex ge.1.17 full
```

Enabling / Disabling Jumbo Frame Support

Purpose

To review, enable, and disable jumbo frame support on one or more ports. This allows Gigabit Ethernet ports to transmit frames up to 10 KB in size.

Commands

For information about...	Refer to page...
show port jumbo	7-14
set port jumbo	7-15
clear port jumbo	7-15

show port jumbo

Use this command to display the status of jumbo frame support and maximum transmission units (MTU) on one or more ports.

Syntax

show port jumbo [*port-string*]

Parameters

port-string	(Optional) Displays the status of jumbo frame support for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, jumbo frame support status for all ports will display.

Mode

Switch command, read-only.

Example

This example shows how to display the status of jumbo frame support for `ge.1.1`:

```
C3(su)->show port jumbo ge.1.1

Port Number   Jumbo Status    Max Frame Size
------------- --------------- ------------------
ge.1.1        Enable          9216
```

set port jumbo

Use this command to enable or disable jumbo frame support on one or more ports.

Syntax

set port jumbo {**enable** | **disable**}[*port-string*]

Parameters

enable | **disable**	Enables or disables jumbo frame support.
port-string	(Optional) Specifies the port(s) on which to disable or enable jumbo frame support. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, jumbo frame support will be enabled or disabled on all ports.

Mode

Switch command, read-write.

Example

This example shows how to enable jumbo frame support for Gigabit Ethernet port 14 in unit/slot 3:

```
C3(su)->set port jumbo enable ge.3.14
```

clear port jumbo

Use this command to reset jumbo frame support status to enabled on one or more ports.

Syntax

clear port jumbo [*port-string*]

Parameters

port-string	(Optional) Specifies the port(s) on which to reset jumbo frame support status to enabled. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, jumbo frame support status will be reset on all ports.

Mode

Switch command, read-write.

Example

This example shows how to reset jumbo frame support status for Gigabit Ethernet port 14 in slot 3:

```
C3(su)->clear port jumbo ge.3.14
```

Setting Auto-Negotiation and Advertised Ability

Purpose

To review, disable or enable auto-negotiation, and to configure port advertisement for speed and duplex.

During auto-negotiation, the port "tells" the device at the other end of the segment what its capabilities and mode of operation are. If auto-negotiation is disabled, the port reverts to the values specified by default speed, default duplex, and the port flow control commands.

In normal operation, with all capabilities enabled, advertised ability enables a port to "advertise" that it has the ability to operate in any mode. The user may choose to configure a port so that only a portion of its capabilities are advertised and the others are disabled.

Note: Advertised ability can be activated only on ports that have auto-negotiation enabled.

Commands

For information about...	Refer to page...
show port negotiation	7-16
set port negotiation	7-17
show port advertise	7-17
set port advertise	7-18
clear port advertise	7-19
show port mdix	7-20
set port mdix	7-20

show port negotiation

Use this command to display the status of auto-negotiation for one or more ports.

Syntax

`show port negotiation` [*`port-string`*]

Parameters

port-string	(Optional) Displays auto-negotiation status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, auto-negotiation status for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display auto-negotiation status for 1-Gigabit Ethernet port 14 in slot 3:

```
C3(su)->show port negotiation ge.3.14
auto-negotiation is enabled on port ge.3.14.
```

set port negotiation

Use this command to enable or disable auto-negotiation on one or more ports.

Syntax

set port negotiation *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) for which to enable or disable auto-negotiation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
enable | **disable**	Enables or disables auto-negotiation.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to disable auto-negotiation on 1-Gigabit Ethernet port 3 in slot 14:

```
C3(su)->set port negotiation ge.3.14 disable
```

show port advertise

Use this command to display port capability and advertisement as far as speed and duplex for auto-negotiation.

Syntax

show port advertise [*port-string*]

Parameters

port-string	(Optional) Displays advertised ability for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, advertisement for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display advertisement status for Gigabit ports 13 and 14:

```
C3(su)->show port advertise ge.1.13-14
ge.1.13      capability    advertised     remote
-----------------------------------------------
10BASE-T        yes           yes          yes
10BASE-TFD      yes           yes          yes
100BASE-TX      yes           yes          yes
100BASE-TXFD    yes           yes          yes
1000BASE-T      no            no           no
1000BASE-TFD    yes           yes          yes
pause           yes           yes          no

ge.1.14      capability    advertised     remote
-----------------------------------------------
10BASE-T        yes           yes          yes
10BASE-TFD      yes           yes          yes
100BASE-TX      yes           yes          yes
100BASE-TXFD    yes           yes          yes
1000BASE-T      no            no           no
1000BASE-TFD    yes           yes          yes
pause           yes           yes          no
```

set port advertise

Use this command to configure what a port will advertise for speed/duplex capabilities in auto-negotiation.

Syntax

set port advertise {*port-string*}{**10t** | **10tfd** | **100tx** | **100txfd** | **1000t** | **1000tfd** | **pause**}

Parameters

port-string	Select the ports for which to configure advertisements. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
10t	Advertise 10BASE-T half duplex mode.
10tfd	Advertise 10BASE-T full duplex mode.
100tx	Advertise 100BASE-TX half duplex mode.
100txfd	Advertise 100BASE-TX full duplex mode.
1000t	Advertise 1000BASE-T half duplex mode.
1000tfd	Advertise 1000BASE-T full duplex mode.
pause	Advertise PAUSE for full-duplex links.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to configure port 1 to advertise 1000BASE-T full duplex:

```
C3(su)->set port advertise ge.1.1 1000tfd
```

clear port advertise

Use this command to configure a port to not advertise a specific speed/duplex capability when auto-negotiating with another port.

Syntax

clear port advertise {*port-string*}{**10t** | **10tfd** | **100tx** | **100txfd** | **1000t** | **1000tfd** | **pause**}

Parameters

port-string	Clear advertisements for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
10t	Do not advertise 10BASE-T half duplex mode.
10tfd	Do not advertise 10BASE-T full duplex mode.
100tx	Do not advertise 100BASE-TX half duplex mode.
100txfd	Do not advertise 100BASE-TX full duplex mode.
1000t	Do not advertise 1000BASE-T half duplex mode.
1000tfd	Do not advertise 1000BASE-T full duplex mode.
pause	Do not advertise PAUSE for full-duplex links.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to configure port 1 to not advertise 10 MB capability for auto-negotiation:

```
C3(su)->clear port advertise ge.1.1 10t 10tfd
```

show port mdix

Use this command to display the status of cable connection type configuration mode for one or more ports. Switch ports can automatically detect and configure the required cable type, either straight through (MDI) or cross-over (MDIX), or the ports can be configured to only allow one type of cable type, either MDI or MDIX.

Syntax

show port mdix {**all**|**auto**|**forced-auto**|**mdi**|**mdix**} [*port-string*]

Parameters

all	Display information about all ports.
auto	Display information about the ports configured to automatically determine the required MDI/MDIX mode.
forced-auto	Display information about the ports forced automatically to determine the required MDI/MDIX mode.
mdi	Display information about the ports configured with MDI only mode.
mdix	Display information about the ports configured with MDIX only mode.
port-string	(Optional) Display the selected MDI/MDIX mode only for the port or ports specified.

Defaults

If *port-string* is not specified, information is displayed for all ports.

Mode

Switch command, read-only.

Example

This example displays information about ports configured for MDIX only mode.

```
C3(su)->show port mdix mdix

 Port Number   MDIX Mode
------------- ------------------
ge.1.27        MDIX
ge.1.28        MDIX
```

set port mdix

Use this command to configure cable connection type configuration mode for one or more ports.

Syntax

set port mdix {**auto**|**forced-auto**|**mdi**|**mdix**} [*port-string*]

Parameters

auto	Configure ports to automatically determine the required MDI/MDIX mode. This is the default condition.
forced-auto	Force ports to automatically determine the required MDI/MDIX mode.

mdi	Configure ports to use MDI mode only.
mdix	Configure ports to use MDIX mode only.
port-string	(Optional) Specify the port or ports to configure.

Defaults

If *port-string* is not entered, all ports on the switch are configured.

Mode

Switch command, read-write.

Usage

By default, Enterasys Networks switch devices are configured to automatically detect the cable type connection, straight through (MDI) or cross-over (MDIX), required by the cable connected to the port. You can configure ports to only use MDI or MDIX connections with this command.

This command only configures Ethernet ports, and cannot be used to configure combo ports on the switch.

Example

This example configures ports ge.1.1 and ge.1.2 to use MDIX mode.

```
C3(su)->set port mdix mdix ge.1.1-2
```

Setting Flow Control

Purpose

To review, enable or disable port flow control. Flow control is used to manage the transmission between two devices as specified by IEEE 802.3x to prevent receiving ports from being overwhelmed by frames from transmitting devices.

Commands

For information about...	Refer to page...
show flowcontrol	7-22
set flowcontrol	7-22

show flowcontrol

Use this command to display the flow control state.

Syntax

show flowcontrol

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the port flow control state:

```
C3(su)->show flowcontrol
Flow control status: enabled
```

set flowcontrol

Use this command to enable or disable flow control.

Syntax

set flowcontrol {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables flow control settings.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to enable flow control:

```
C3(su)->set flowcontrol enable
```

Setting Port Link Traps and Link Flap Detection

Purpose

To disable or re-enable link traps, display link trap status, and to configure the link flapping detection function. By default, all ports are enabled to send SNMP trap messages indicating changes to their link status (up or down).

The link flap function detects when a link is going up and down rapidly (also called "link flapping") on a physical port, and takes the required actions (disable port, and eventually send notification trap) to stop such a condition. If left unresolved, the "link flapping" condition can be detrimental to network stability because it can trigger Spanning Tree and routing table recalculation.

Commands

show port trap

Use this command to display whether the port is enabled for generating an SNMP trap message if its link state changes.

Syntax

`show port trap` [*`port-string`*]

Parameters

port-string	(Optional) Displays link trap status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, the trap status for all ports will be displayed.

Mode

Switch command, read-write.

Example

This example shows how to display link trap status for ge.3.1 through 4:

```
C3(su)->show port trap ge.3.1-4
Link traps enabled on port ge.3.1.
Link traps enabled on port ge.3.2.
Link traps enabled on port ge.3.3.
Link traps enabled on port ge.3.4.
```

set port trap

Use this command to enable of disable ports for sending SNMP trap messages when their link status changes.

Syntax

set port trap *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) for which to enable or disable port traps. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
enable | **disable**	Enables or disables sending trap messages when link status changes.

Defaults

Sending traps when link status changes is enabled by default.

Mode

Switch command, read-write.

Example

The following example disables sending trap on ge.3.1.

```
C3(su)->set port trap ge.3.1 disable
```

show linkflap

Use this command to display link flap detection state and configuration information.

Syntax

show linkflap {**globalstate** | **portstate** | **parameters** | **metrics** | **portsupported** | **actsupported** | **maximum** | **downports** | **action** | **operstatus** | **threshold** | **interval**] | **downtime** | **currentcount** | **totalcount** | **timelapsed** | **violations** [*port-string*]}

Parameters

globalstate	Displays the global enable state of link flap detection.
portstate	Displays the port enable state of link flap detection.
parameters	Displays the current value of settable link flap detection parameters.
metrics	Displays linkflap detection metrics.
portsupported	Displays ports which can support the link flap detection function.
actsupported	Displays link flap detection actions supported by system hardware.
maximum	Displays the maximum allowed linkdowns per 10 seconds supported by system hardware.
downports	Displays ports disabled by link flap detection due to a violation.
action	Displays linkflap actions taken on violating port(s).
operstatus	Displays whether linkflap has deactivated port(s).
threshold	Displays the number of allowed link down transitions before action is taken.
interval	Displays the time period for counting link down transitions.
downtime	Displays how long violating port(s) are deactivated.
currentcount	Displays how many linkdown transitions are in the current interval.
totalcount	Displays how many linkdown transitions have occurred since the last reset.
timelapsed	Displays the time period since the last link down event or reset.
violations	Displays the number of link flap violations since the last reset.
port-string	(Optional) Displays information for specific port(s).

Defaults

- If not specified, information about all link flap detection settings will be displayed.
- If *port-string* is not specified, information for all ports will be displayed.

Mode

Switch mode, read-only.

Usage

The linkflap default conditions are shown in the following table.

Linkflap Parameter	Default Condition
Linkflap global state	Disabled
Linkflap port state	Disabled
Linkflap action	None
Linkflap interval	5
Linkflap maximum allowed link downs per 10 seconds	20
Linkflap threshold (number of allowed link down transitions before action is taken)	10

Examples

This example shows how to display the global status of the link trap detection function:

```
C3(rw)->show linkflap globalstate
Linkflap feature globally disabled
```

This example shows how to display ports disabled by link flap detection due to a violation:

```
C3(rw)->show linkflap downports
Ports currently held DOWN for Linkflap violations:
None.
```

This example shows how to display the link flap parameters table:

```
C3(rw)->show linkflap parameters
Linkflap Port Settable Parameter Table (X means error occurred)
Port      LF Status  Actions  Threshold   Interval    Downtime
--------  ---------  -------  ----------  ----------  ----------
ge.1.1    disabled   .......  10          5           300
ge.1.2    enabled    D..S..T  3           5           300
ge.1.3    disabled   ...S..T  10          5           300
```

Table 7-4 provides an explanation of the **show linkflap parameters** command output.

Table 7-4 show linkflap parameters Output Details

Output Field	What it displays...
Port	Port designation.
LF Status	Link flap enabled state.
Actions	Actions to be taken if the port violates allowed link flap behavior. D = disabled, S = Syslog entry will be generated, T= SNMP trap will be generated.
Threshold	Number of link down transitions necessary to trigger the link flap action.
Interval	Time interval (in seconds) for accumulating link down transitions.
Downtime	Interval (in seconds) port(s) will be held down after a link flap violation.

This example shows how to display the link flap metrics table:

```
C3(rw)->show linkflap metrics
Port      LinkStatus   CurrentCount  TotalCount  TimeElapsed  Violations
--------  -----------  ------------  ----------  -----------  -------------
ge.1.1    operational  0             0           241437       0
ge.1.2    disabled     4             15          147          5
ge.1.3    operational  3             3           241402       0
```

Table 7-5 provides an explanation of the **show linkflap metrics** command output.

Table 7-5 show linkflap metrics Output Details

Output Field	What it displays...
Port	Port designation.
LinkStatus	Link status according to the link flap function.
CurrentCount	Link down count accruing toward the link flap threshold.
TotalCount	Number of link downs since system start,

Table 7-5 show linkflap metrics Output Details (Continued)

Output Field	What it displays...
TimeElapsed	Time (in seconds) since the last link down event.
Violations	Number of link flap violations on listed ports since system start.

set linkflap globalstate

Use this command to globally enable or disable the link flap detection function.

Syntax

set linkflap globalstate {**disable** | **enable**}

Parameters

disable | **enable**	Globally disables or enables the link flap detection function.

Defaults

By default, the function is disabled globally and on all ports.

Mode

Switch mode, read-write.

Usage

By default, the function is disabled globally and on all ports. If disabled globally after per-port settings have been configured using the linkflap commands, per-port settings will be retained.

Example

This example shows how to globally enable the link trap detection function.

```
C3(rw)->set linkflap globalstate enable
```

set linkflap portstate

Use this command to enable or disable link flap monitoring on one or more ports.

Syntax

set linkflap portstate {**disable** | **enable**} [*port-string*]

Parameters

disable | **enable**	Disables or enables the link flap detection function.
port-string	(Optional) Specifies the port or ports on which to disable or enable monitoring.

Defaults

If *port-string* is not specified, all ports are enabled or disabled.

Mode

Switch command, read-write.

Example

This example shows how to enable the link trap monitoring on all ports.

```
C3(rw)->set linkflap portstate enable
```

set linkflap interval

Use this command to set the time interval (in seconds) for accumulating link down transitions.

Syntax

set linkflap interval *port-string interval-value*

Parameters

port-string	Specifies the port(s) on which to set the link flap interval.
interval-value	Specifies an interval in seconds. A value of 0 will set the interval to forever.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the link flap interval on port ge.1.4 to 1000 seconds.

```
C3(rw)->set linkflap interval ge.1.4 1000
```

set linkflap action

Use this command to set reactions to a link flap violation.

Syntax

set linkflap action *port-string* {**disableInterface** | **gensyslogentry** | **gentrap** | **all**}

Parameters

port-string	Specifies the port(s) on which to set the link flap action.
disableInterface	Sets the reaction as disabling the interface.
gensyslogentry	Sets the reaction as generating a syslog entry.
gentrap	Sets the reaction as generating an SNMP trap.
all	Sets the reaction as all of the above.

Defaults

None.

Mode

Switch mode, read-write.

Example

This example shows how to set the link flap violation action on port ge.1.4 to generating a Syslog entry.

```
C3(rw)->set linkflap action ge.1.4 gensyslogentry
```

clear linkflap action

Use this command to clear reactions to a link flap violation.

Syntax

clear linkflap action [*port-string*] {**disableInterface** | **gensyslogentry** | **gentrap** | **all**}

Parameters

port-string	(Optional) Specifies the port(s) on which to clear the link flap action.
disableInterface	Clears the reaction as disabling the interface.
gensyslogentry	Clears the reaction as generating a syslog entry.
gentrap	Clears the reaction as generating an SNMP trap.
all	Clears the reaction as all of the above.

Defaults

If *port-string* is not specified, actions will be cleared on all ports.

Mode

Switch mode, read-write.

Example

This example shows how to clear the link flap violation action on port ge.1.4 to generating a Syslog entry.

```
C3(rw)->clear linkflap action ge.1.4 gensyslogentry
```

set linkflap threshold

Use this command to set the link flap action trigger count.

Syntax

set linkflap threshold *port-string threshold-value*

Parameters

port-string	Specifies the port(s) on which to set the link flap action trigger count.
threshold-value	Specifies the number of link down transitions necessary to trigger the link flap action. A minimum of 1 must be configured.

Defaults

None.

Mode

Switch mode, read-write.

Example

This example shows how to set the link flap threshold on port ge.1.4 to 5.

```
C3(rw)->set linkflap threshold ge.1.4 5
```

set linkflap downtime

Use this command to set the time interval (in seconds) one or more ports will be held down after a link flap violation.

Syntax

`set linkflap downtime` *`port-string downtime-value`*

Parameters

port-string	Specifies the port(s) on which to set the link flap downtime.
downtime-value	Specifies a downtime in seconds. A value of 0 will set the downtime to forever.

Defaults

None.

Mode

Switch mode, read-write.

Example

This example shows how to set the link flap downtime on port ge.1.4 to 5000 seconds.

```
C3(rw)->set linkflap downtime ge.1.4 5000
```

clear linkflap down

Use this command to toggle link flap disabled ports to operational.

Syntax

`clear linkflap down` [*`port-string`*]

Parameters

port-string	(Optional) Specifies the ports to make operational.

Defaults

If *port-string* is not specified, all ports disabled by a link flap violation will be made operational.

Mode

Switch mode, read-write.

Example

This example shows how to make disabled port ge.1.4 operational.

```
C3(rw)->clear linkflap down ge.1.4
```

clear linkflap

Use this command to clear all link flap options and / or statistics on one or more ports.

Syntax

clear linkflap {**all** | **stats** [*port-string*] | **parameter** *port-string* {**threshold** | **interval** | **downtime** | **all**}

Parameters

all | **stats**	Clears all options and statistics, or clears only statistics.
parameter	Clears link flap parameters.
threshold | **interval** | **downtime** | **all**	Clears link flap threshold, interval, downtime or all parameters.
port-string	(Optional unless parameter is specified) Specifies the port(s) on which to clear settings.

Defaults

If *port-string* is not specified, settings and/or statistics will be cleared on all ports.

Mode

Switch mode, read-write.

Example

This example shows how to clear all link flap options on port ge.1.4.

```
C3(rw)->clear linkflap all ge.1.4
```

Configuring Broadcast Suppression

Purpose

To review and set the broadcast suppression threshold for one or more ports. This feature limits the number of received broadcast frames the switch will accept per port. Broadcast suppression thresholds apply only to broadcast traffic—multicast traffic is not affected. By default, a broadcast suppression threshold of 14881 packets per second (pps) will be used, regardless of actual port speed. Broadcast suppression protects against broadcast storms and ARP sweeps.

Note: Class of Service functionality can also be used to control broadcast, unknown unicast, and/or multicast flooding. This feature prevents configured ports from being disrupted by a traffic storm by rate-limiting specific types of packets through those ports. Refer to "About CoS-Based Flood Control" on page 10-20 for more information.

Commands

For information about...	Refer to page...
show port broadcast	7-33
set port broadcast	7-34
clear port broadcast	7-34

show port broadcast

Use this command to display port broadcast suppression thresholds.

Syntax

show port broadcast [*port-string*]

Parameters

port-string	(Optional) Select the ports for which to show broadcast suppression thresholds. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, broadcast status of all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display the broadcast suppression thresholds for ports 1 through 4:

```
C3(su)->show port broadcast ge.1.1-4
Port          Total BC       Threshold
              Packets        (pkts/s)
--------------------------------------
ge.1.1        0               50
```

```
ge.1.2          0               50
ge.1.3          0               40
ge.1.4          0               14881
```

set port broadcast

Use this command to set the broadcast suppression threshold, in packets per second, on one or more ports. This sets a threshold on the broadcast traffic that is received and switched out to other ports.

Syntax

set port broadcast *port-string threshold-val*

Parameters

port-string	Select the ports for which to configure broadcast suppression thresholds. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
threshold-val	Sets the packets per second threshold on broadcast traffic. Maximum value is • 148810 for Fast Ethernet ports • 1488100 for 1-Gigabit ports. • 14881000 for 10- Gigabit ports

Defaults

None.

Mode

Switch command, read-write.

Usage

Per port broadcast suppression is hardset to be globally enabled on the C3. If you would like to disable broadcast suppression, you can get the same result by setting the threshold limit for each port to the maximum number of packets which can be received per second as listed in the parameters section, above. The default broadcast suppression threshold for all ports is set to 14881.

Example

This example configures ports 1 through 5 with a broadcast limit of 50 pps:

```
C3(su)->set port broadcast ge.1.1-5 50
```

clear port broadcast

Use this command to clear the broadcast threshold limit to the default value of 14881 for the selected port.

Syntax

clear port broadcast *port-string* **threshold**

Parameters

port-string	Select the ports for which to clear broadcast suppression thresholds. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example clears the broadcast threshold limit to 14881 pps for ports 1 through 5:

```
C3(su)->clear port broadcast ge.1.1-5 threshold
```

Port Mirroring

Caution: Port mirroring configuration should be performed only by personnel who are knowledgeable about the effects of port mirroring and its impact on network operation.

The SecureStack C3 device allows you to mirror (or redirect) the traffic being switched on a port for the purposes of network traffic analysis and connection assurance. When port mirroring is enabled, one port becomes a monitor port for another port within the device.

Note: An Enterasys Networks Feature Guide document containing an in-depth discussion of port mirroring configuration is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

Mirroring Features

The SecureStack C3 device supports the following mirroring features:

- Mirroring can be configured in a many-to-one configuration so that one target (destination) port can monitor traffic on up to 8 source ports. Only one mirror destination port can be configured per stack, if applicable.
- Both transmit and receive traffic will be mirrored.
- A destination port will only act as a mirroring port when the session is operationally active.
- When a port mirror is created, the mirror destination port is removed from the egress list of VLAN 1 after a reboot.
- MAC addresses will be learned for packets tagged with the mirror VLAN ID. This will prevent the ability to snoop traffic across multiple hops.

Caution: Traffic mirrored to a VLAN may contain control traffic. This may be interpreted by the downstream neighbor as legal control frames. It is recommended that you disable any protocols (such as Spanning Tree) on inter-switch connections that might be affected .

Remote Port Mirroring

Remote port mirroring is an extension to port mirroring which facilitates simultaneous mirroring of multiple source ports on multiple switches across a network to one or more remote destination ports.

Remote port mirroring involves configuration of the following port mirroring related parameters:

1. Configuration of normal port mirroring source ports and one destination port on all switches, as described above.
2. Configuration of a mirror VLAN, which is a unique VLAN on which mirrored packets traverse across the network. The mirror VLAN has to be configured on ALL switches across the network along which mirrored traffic traverses, from the switch where the source ports reside to the switch where the mirrored packets are sniffed and/or captured.

You must ensure that switches involved are properly configured to facilitate correct remote port mirroring operation. The following points in particular need to be observed:

- On the source switch, the correct destination port must be chosen to ensure that there is an egress path from that port to the desired remote destination(s).
- All ports on the path from the source port to the remote destination must be members of the mirror VLAN.

- On switches on the path from the source port to the remote destination, egress tagging has to be enabled on potential egress ports for the mirror VLAN.

With the introduction of remote port mirroring:

- Configured mirror destination ports will NOT lose their switching or routing properties as they do on SecureStack A2, B2, or C2 products.
- On switches where the mirror VLAN has been configured, any traffic on that VLAN will be flooded on the VLAN. It will never be unicast, even if the source address of the traffic as been learned on the switch.

Configuring SMON MIB Port Mirroring

Overview

SMON port mirroring support allows you to redirect traffic on ports remotely using SMON MIBs. This is useful for troubleshooting or problem solving when network management through the console port, telnet, or SSH is not feasible.

Procedures

Perform the following steps to configure and monitor port mirroring using SMON MIB objects.

To c reate and enable a port mirroring instance:

1. Open a MIB browser, such as Netsight MIB Tools
2. In the MIB directory tree, navigate to the **portCopyEntry** folder and expand it.
3. Select the **portCopyStatus** MIB.
4. Enter a desired source and target port in the **Instance** field using the format *source.target*.

   For example, 3.2 would create a relationship where source port ge.1.3 would be mirrored to target port ge.1.2.

Note: In order to configure a port mirroring relationship, both source and destination interfaces must be enabled and operational (up).

5. Enter MIB option **4** (createAndGo) and perform an SNMP **Set** operation.
6. (Optional) Use the CLI to verify the port mirroring instance has been created and enabled as shown in the following example:

```
C3(su)->show port mirroring
Port Mirroring
==============
Source Port     = ge.1.3
Target Port     = ge.1.2
Frames Mirrored = Rx and Tx
Port Mirroring status enabled
```

To create a port mirroring instance without automatically enabling it:

1. Complete steps 1-4 above.
2. Enter MIB option **5** (createAndWait) and perform an SNMP **Set** operation.
3. (Optional) Use the CLI to verify the port mirroring instance has been created set to disabled mode as shown in the following example:

```
C3(su)->show port mirroring
```

```
Port Mirroring
==============
Source Port     = ge.1.3
Target Port     = ge.1.2
Frames Mirrored = Rx and Tx
Port Mirroring status disabled
```

4. When you are ready to enable this instance, enter MIB option **1** (active) and perform an SNMP **Set** operation.
5. (Optional) Use the CLI to verify the port mirroring instance has been enabled.

To delete a port mirroring instance:

1. Select a previously created port mirroring instance in your MIB browser.
2. Enter MIB option **6** (destroy) and perform an SNMP **Set** operation.
3. (Optional) Use the CLI to verify the port mirroring instance has been deleted as shown in the following example:

```
C3(su)->show port mirroring
No Port Mirrors configured.
```

Purpose

To review and configure port mirroring on the device.

Commands

For information about...	Refer to page...
show port mirroring	7-38
set port mirroring	7-39
clear port mirroring	7-40
set mirror vlan	7-40
clear mirror vlan	7-41

show port mirroring

Use this command to display the source and target ports for mirroring, and whether mirroring is currently enabled or disabled for those ports.

Syntax

`show port mirroring`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display port mirroring information. In this case, ge.1.4 is configured as a source port and ge.1.11 is a target and mirroring has been enabled between these ports:

```
C3(su)->show port mirroring

Port Mirroring
==============
 Source Port = ge.1.4
 Target Port = ge.1.11
 Frames Mirrored = Rx and Tx
 Port Mirroring status enabled.
```

set port mirroring

Use this command to create a new mirroring relationship or to enable or disable an existing mirroring relationship between two ports.

Notes: When a port mirror is created, the mirror destination port is removed from VLAN 1's egress list after a reboot.
"MAC addresses will be learned for packets tagged with the mirror VLAN ID. This will prevent the ability to snoop traffic across multiple hops.

Syntax

set port mirroring {**create** | **disable** | **enable**} *source destination*}

Parameters

create | **disable** | **enable**	Creates, disables or enables mirroring settings on the specified ports. By default, port mirrors are enabled automatically when created.
source	Specifies the source port designation. This is the port on which the traffic will be monitored. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
destination	Specifies the target port designation. This is the port that will duplicate or "mirror" all the traffic on the monitored port. Only one destination port can be configured per stack, if applicable. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

Port mirrors are automatically enabled when created on this platform.

Mode

Switch command, read-write.

Usage

Note that LAG ports and their underlying physical ports, as described in "Link Aggregation Control Protocol (LACP)" on page 7-42, cannot be mirrored.

Example

This example shows how to create and enable port mirroring with ge.1.4 as the source port, and ge.1.11 as the target port:

```
C3(su)->set port mirroring create ge.1.4 ge.1.11
```

clear port mirroring

Use this command to clear a port mirroring relationship.

Syntax

clear port mirroring *source destination*

Parameters

source	Specifies the source port of the mirroring configuration to be cleared. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
destination	Specifies the target port of the mirroring configuration to be cleared.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear a port mirroring relationship between source port ge.1.4 and target port ge.1.11:

```
C3(su)->clear port mirroring ge.1.4 ge.1.11
```

set mirror vlan

Assigns a VLAN to be reserved for mirroring traffic. If a mirrored VLAN is created, all mirrored traffic will egress VLAN tagged. All traffic on the mirror VLAN will be flooded.

Syntax

set mirror vlan *vlan-id*

Parameters

vlan-id	Specifies the VLAN to be used for remote port mirroring. The ID can range from 2 to 4093.

Defaults

None.

Mode

Switch command, read-write.

Usage

Refer to "Remote Port Mirroring" on page 7-36 for information about configuring mirror VLANs.

Use the **show port mirroring** command to display the VLANs configured for remote port mirroring.

Example

The following example assigns a VLAN for mirroring traffic and then shows the configured port mirroring with the **show port mirror** command.

```
C3(su)->set mirror vlan 2

C3(su)->show port mirroring
Port Mirroring
==============
Source Port     = ge.1.1
Target Port     = ge.1.10
Frames Mirrored = Rx and Tx
Port Mirroring status enabled

Mirror Vlan     = 2
```

clear mirror vlan

Use this command to clear the VLAN to be reserved for mirroring traffic.

Syntax

clear mirror vlan *vlan-id*

Parameters

vlan-id	Specifies the VLAN to be cleared. The ID can range from 2 to 4093.

Defaults

None.

Mode

Switch command, read-write.

Example

The following example clears VLAN 2 from being used for remote port mirroring.

```
C3(su)->clear mirror vlan 2
```

Link Aggregation Control Protocol (LACP)

Caution: Link aggregation configuration should only be performed by personnel who are knowledgeable about Spanning Tree and Link Aggregation, and fully understand the ramifications of modifications beyond device defaults. Otherwise, the proper operation of the network could be at risk.

Using multiple links simultaneously to increase bandwidth is a desirable switch feature, which can be accomplished if both sides agree on a set of ports that are being used as a Link Aggregation Group (LAG). Once a LAG is formed from selected ports, problems with looping can be avoided since the Spanning Tree can treat this LAG as a single port.

Enabled by default, the Link Aggregation Control Protocol (LACP) logically groups interfaces together to create a greater bandwidth uplink, or link aggregation, according to the IEEE 802.3ad standard. This standard allows the switch to determine which ports are in LAGs and configure them dynamically. Since the protocol is based on the IEEE 802.3ad specification, any switch from any vendor that supports this standard can aggregate links automatically.

802.3ad LACP aggregations can also be run to end-users (that is, a server) or to a router.

Note: Earlier (proprietary) implementations of port aggregation referred to groups of aggregated ports as “trunks”.

LACP Operation

For each aggregatable port in the device, LACP:

- Maintains configuration information (reflecting the inherent properties of the individual links as well as those established by management) to control aggregation.
- Exchanges configuration information with other devices to allocate the link to a Link Aggregation Group (LAG).

Note: A given link is allocated to, at most, one Link Aggregation Group (LAG) at a time. The allocation mechanism attempts to maximize aggregation, subject to management controls.

- Attaches the port to the aggregator used by the LAG, and detaches the port from the aggregator when it is no longer used by the LAG.
- Uses information from the partner device’s link aggregation control entity to decide whether to aggregate ports.

The operation of LACP involves the following activities:

- Checking that candidate links can actually be aggregated.
- Controlling the addition of a link to a LAG, and the creation of the group if necessary.
- Monitoring the status of aggregated links to ensure that the aggregation is still valid.
- Removing a link from a LAG if its membership is no longer valid, and removing the group if it no longer has any member links.

In order to allow LACP to determine whether a set of links connect to the same device, and to determine whether those links are compatible from the point of view of aggregation, it is necessary to be able to establish

- A globally unique identifier for each device that participates in link aggregation.

- A means of identifying the set of capabilities associated with each port and with each aggregator, as understood by a given device.
- A means of identifying a LAG and its associated aggregator.

Note: The path cost of a LAG port will be displayed as zero when it is not an active link.

LACP Terminology

Table 7-6 defines key terminology used in LACP configuration.

Table 7-6 LACP Terms and Definitions

Term	Definition
Aggregator	Virtual port that controls link aggregation for underlying physical ports. Each SecureStack C3 module provides 6 aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.6**.
LAG	Link Aggregation Group. Once underlying physical ports (for example, fe**.x.x**) are associated with an aggregator port, the resulting aggregation will be represented as one LAG with a **lag.x.x** port designation. SecureStack C3 LAGs can have up to 8 associated physical ports.
LACPDU	Link Aggregation Control Protocol Data Unit. The protocol exchanges aggregation state/mode information by way of a port's actor and partner operational states. LACPDUs sent by the first party (the actor) convey to the second party (the actor's protocol partner) what the actor knows, both about its own state and that of its partner.
Actor and Partner	An actor is the local device sending LACPDUs. Its protocol partner is the device on the other end of the link aggregation. Each maintains current status of the other via LACPDUs containing information about their ports' LACP status and operational state.
Admin Key	Value assigned to aggregator ports and physical ports that are candidates for joining a LAG. The LACP implementation on SecureStack C3 devices will use this value to form an oper key and will determine which underlying physical ports are capable of aggregating by comparing oper keys. Aggregator ports allow only underlying ports with oper keys matching theirs to join their LAG. On SecureStack C3 devices, the default admin key value is 32768.
System Priority	Value used to build a LAG ID, which determines aggregation precedence. If there are two partner devices competing for the same aggregator, LACP compares the LAG IDs for each grouping of ports. The LAG with the lower LAG ID is given precedence and will be allowed to use the aggregator. **Note:** Only one LACP system priority can be set on a SecureStack C3 device, using either the **set lacp asyspri** command (page 7-47), or the **set port lacp** command (page 7-52).

SecureStack C3 Usage Considerations

In normal usage (and typical implementations) there is no need to modify any of the default LACP parameters on the switch. The default values will result in the maximum number of aggregations possible. If the switch is placed in a configuration with its peers not running the protocol, no dynamic link aggregations will be formed and the switch will function normally (that

is, will block redundant paths). For information about building static aggregations, refer to **set lacp static** (page 7-48).

Each SecureStack C3 module provides six virtual link aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.6**. Each LAG can have up to eight associated physical ports. Once underlying physical ports (for example, **fe.x.x**, or **ge.x.x**) are associated with an aggregator port, the resulting aggregation will be represented as one LAG with a **lag.0.x** port designation. LACP determines which underlying physical ports are capable of aggregating by comparing operational keys. Aggregator ports allow only underlying ports with keys matching theirs to join their LAG.

LACP uses a system priority value to build a LAG ID, which determines aggregation precedence. If there are two partner devices competing for the same aggregator, LACP compares the LAG IDs for each grouping of ports. The LAG with the lower LAG ID is given precedence and will be allowed to use the aggregator.

There are a few cases in which ports will not aggregate:

- An underlying physical port is attached to another port on this same switch (loopback).
- There is no available aggregator for two or more ports with the same LAG ID. This can happen if there are simply no available aggregators, or if none of the aggregators have a matching admin key and system priority.
- 802.1x authentication is enabled using the **set eapol** command (page 16-18) and ports that would otherwise aggregate are not 802.1X authorized.

The LACP implementation on the SecureStack C3 device will allow up to eight physical ports into a LAG. The device with the lowest LAG ID determines which underlying physical ports are allowed into a LAG based on the ports' LAG port priority. Ports with the lowest LAG port priority values are allowed into the LAG and all other speed groupings go into a standby state.

Multi-port LAGs will continue to operate as long as there is at least one active port in the LAG. Therefore, there is no need to create backup single port LAGs or to specifically assign the LAG and all its physical ports to the egress list of the LAG's VLAN.

Typically, two or more ports are required to form a LAG. However, you can enable the creation of single port LAGs as described in "set lacp singleportlag" on page 7-50. If a single port LAG goes down and the switch stays up, the switch will reconfigure the LAG to the same LAG number if the port comes back up.

Note: To aggregate, underlying physical ports must be running in full duplex mode and must be of the same operating speed.

Commands

For information about...	Refer to page...
show lacp	7-45
set lacp	7-46
set lacp asyspri	7-47
set lacp aadminkey	7-47
clear lacp	7-48
set lacp static	7-48
clear lacp static	7-49

show lacp

Use this command to display information about one or more aggregator ports.

Syntax

show lacp [*port-string*]

Parameters

port-string	(Optional) Displays LACP information for specific LAG port(s). Valid port designations are lag.0.1 - 6.

Defaults

If *port-string* is not specified, link aggregation information for all LAGs will be displayed.

Mode

Switch command, read-only.

Usage

Each SecureStack C3 module provides 6 virtual link aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.6**. Once underlying physical ports (that is, **ge.x.x**) are associated with an aggregator port, the resulting aggregation will be represented as one Link Aggregation Group (LAG) with a **lag.x.x** port designation.

Example

This example shows how to display lacp information for lag.0.1. The following table describes the output fields.

```
C3(su)->show lacp lag.0.1
Global Link Aggregation state: enabled
Single Port LAGs:              disabled

Aggregator: lag.0.1
                         Actor                  Partner
System Identifier:     00:01:F4:5F:1E:20    00:11:88:11:74:F9
  System Priority:                 32768                32768
        Admin Key:                 32768
         Oper Key:                 32768                    0
   Attached Ports:    ge.1.1
                      ge.1.3
```

Table 7-7 provides an explanation of the command output.

Table 7-7 show lacp Output Details

Output Field	What It Displays...
Global Link Aggregation state	Shows if LACP is enabled or disabled on the switch.
Single Port LAGs	Displays if the single port LAG feature has been enabled on the switch. See "set lacp singleportlag" on page 7-50 for more about single port LAG.
Aggregator	LAG port designation. Each SecureStack C3 module provides 6 virtual link aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.6**. Once underlying physical ports (for example, fe**.x.x**) are associated with an aggregator port, the resulting Link Aggregation Group (LAG) is represented with a **lag.x.x** port designation.
Actor	Local device participating in LACP negotiation.
Partner	Remote device participating in LACP negotiation.
System Identifier	MAC addresses for actor and partner.
System Priority	System priority value which determines aggregation precedence. Only one LACP system priority can be set on a SecureStack C3 device, using either the **set lacp asyspri** command (page 7-47), or the **set port lacp** command (page 7-52).
Admin Key	Port's assigned key. SecureStack C3 devices provide a default admin key value of 32768 for all LAG ports (lag.0.1 though lag.0.6).
Oper Key	Port's operational key, derived from the admin key. Only underlying physical ports with oper keys matching the aggregator's will be allowed to aggregate.
Attached Ports	Underlying physical ports associated with this aggregator.

set lacp

Use this command to disable or enable the Link Aggregation Control Protocol (LACP) on the device.

Syntax

```
set lacp {disable | enable}
```

Parameters

disable | **enable**	Disables or enables LACP.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to disable LACP:

```
C3(su)->set lacp disable
```

set lacp asyspri

Use this command to set the LACP system priority.

Syntax

set lacp asyspri *value*

Parameters

asyspri	Sets the system priority to be used in creating a LAG (Link Aggregation Group) ID. Valid values are **0** to **65535**.
value	Specifies a system priority value. Valid values are **0** to **65535**, with precedence given to lower values.

Defaults

None.

Mode

Switch command, read-write.

Usage

LACP uses this value to determine aggregation precedence. If there are two partner devices competing for the same aggregator, LACP compares the LAG IDs for each grouping of ports. The LAG with the lower LAG ID is given precedence and will be allowed to use the aggregator.

Example

This example shows how to set the LACP system priority to 1000:

```
C3(su)->set lacp asyspri 1000
```

set lacp aadminkey

Use this command to set the administratively assigned key for one or more aggregator ports.

Syntax

set lacp aadminkey *port-string value*

Parameters

port-string	Specifies the LAG port(s) on which to assign an admin key.
value	Specifies an admin key value to set. Valid values are **0** to **65535**. The default admin key value is 32768.

Defaults

None.

Mode

Switch command, read-write.

Usage

LACP will use this value to form an oper key. Only underlying physical ports with oper keys matching those of their aggregators will be allowed to aggregate. The default admin key value for all LAG ports is 32768.

Example

This example shows how to set the LACP admin key to 2000 for LAG port 6:

```
C3(su)->set lacp aadminkey lag.0.6 2000
```

clear lacp

Use this command to clear LACP system priority or admin key settings.

Syntax

clear lacp {[**asyspri**] [**aadminkey** *port-string*]}

Parameters

asyspri	Clears system priority.
aadminkey *port-string*	Resets admin keys for one or more ports to the default value of 32768.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the actor admin key for LAG port 6:

```
C3(su)->clear lacp aadminkey lag.0.6
```

set lacp static

Use this command to disable or enable static link aggregation, or to assign one or more underlying physical ports to a Link Aggregation Group (LAG).

Syntax

set lacp static {disable | enable} | *lagportstring* [*key*] *port-string*

Parameters

disable | **enable**	Disables or enables static link aggregation.
lagportstring	Specifies the LAG aggregator port to which new ports will be assigned.

key	(Optional) Specifies the new member port and LAG port aggregator admin key value. Only ports with matching keys are allowed to aggregate. Valid values are **0** - **65535**.  **Note:** This key value must be unique. If ports other than the desired underlying physical ports share the same admin key value, aggregation will fail or undesired aggregations will form.
port-string	Specifies the member port(s) to add to the LAG. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If not specified, a *key* will be assigned according to the specified aggregator. For example a key of 4 would be assigned to lag.0.4.

Mode

Switch command, read-write.

Example

This example shows how to add port ge.1.6 to the LAG of aggregator port 6:

```
C3(su)->set lacp static lag.0.6 ge.1.6
```

clear lacp static

Use this command to remove specific ports from a Link Aggregation Group.

Syntax

`clear lacp static` *`lagportstring port-string`*

Parameters

lagportstring	Specifies the LAG aggregator port from which ports will be removed.
port-string	Specifies the port(s) to remove from the LAG. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to remove ge.1.6 from the LAG of aggregator port 6:

```
C3(su)->clear lacp static lag.0.6 ge.1.6
```

set lacp singleportlag

Use this command to enable or disable the formation of single port LAGs.

Syntax

```
set lacp singleportlag {enable | disable}
```

Parameters

disable | **enable**	Enables or disables the formation of single port LAGs.

Defaults

None.

Mode

Switch command, read-write.

Usage

When single port LAGs are enabled, Link Aggregration Groups can be formed when only one port is receiving protocol transmissions from a partner. When this setting is disabled, two or more ports are required to form a LAG.

This setting has no effect on existing LAGs created with multiple member ports. It also does not prevent previously formed LAGs from coming up after they have gone down, as long as any previous LAG member ports come up connected to the same switch as before the LAG went down.

Example

This example enables the formation of single port LAGs:

```
C3(su)->set lacp singleportlag enable
```

clear lacp singleportlag

Use this command to reset the single port LAG function back to the default state of disabled.

Syntax

```
clear lacp singleportlag
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the single port LAG function back to disabled:

```
C3(su)->clear lacp singleportlag
```

show port lacp

Use this command to display link aggregation information for one or more underlying physical ports.

Syntax

show port lacp port *port-string* {[**status {detail | summary}**] | [**counters**]}

Parameters

port *port-string*	Displays LACP information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
status detail | **summary**	Displays LACP status in detailed or summary information.
counters	Displays LACP counter information.

Defaults

None.

Mode

Switch command, read-only.

Usage

State definitions, such as ActorAdminState and Partner AdminState, are indicated with letter abbreviations. If the **show port lacp** command displays one or more of the following letters, it means the state is true for the associated actor or partner ports:

- **E** = Expired
- **F** = Defaulted
- **D** = Distributing (tx enabled)
- **C** = Collecting (rx enabled)
- **S** = Synchronized (actor and partner agree)
- **G** = Aggregation allowed
- **S/l** = Short/Long LACP timeout
- **A/p** = Active/Passive LACP

For more information about these states, refer to **set port lacp** (page 7-52) and the IEEE 802.3 2002 specification.

Examples

This example shows how to display detailed LACP status information for port ge.1.12:

```
C3(su)-> show port lacp port ge.1.12 status detail
```

```
Port Instance:                ge.1.12
ActorPort:                      1411  PartnerAdminPort:                    1411
ActorSystemPriority:           32768  PartnerOperPort:                     1411
ActorPortPriority:             32768  PartnerAdminSystemPriority:         32768
ActorAdminKey:                 32768  PartnerOperSystemPriority:          32768
ActorOperKey:                  32768  PartnerAdminPortPriority:           32768
ActorAdminState:             -----GlA  PartnerOperPortPriority:            32768
ActorOperState:              -F----lA  PartnerAdminKey:                     1411
ActorSystemID:    00-e0-63-9d-b5-87  PartnerOperKey:                      1411
SelectedAggID:                  none  PartnerAdminState:               --DCSGlp
AttachedAggID:                  none  PartnerOperState:                --DC-Glp
MuxState:                   Detached  PartnerAdminSystemID:   00-00-00-00-00-00
DebugRxState:          port Disabled  PartnerOperSystemID:    00-00-00-00-00-00
```

This example shows how to display summarized LACP status information for port ge.1.12:

```
C3(su)->show port lacp port ge.1.12 status summary
Port     Aggr        Actor System           Partner System
                  Pri:   System ID:  Key:    Pri: System ID:     Key:
ge.1.12    none [(32768,00e0639db587,32768),(32768,000000000000, 1411)]
```

This example shows how to display LACP counters for port ge.1.12:

```
C3(su)->show port lacp port ge.1.12 counters
Port Instance:                       ge.1.12
LACPDUsRx:                           11067
LACPDUsTx:                               0
IllegalRx:                               0
UnknownRx:                               0
MarkerPDUsRx:                            0
MarkerPDUsTx:                            0
MarkerResponsePDUsRx:                    0
MarkerResponsePDUsTx:                  374
```

set port lacp

Use this command to set link aggregation parameters for one or more ports. These settings will determine the specified underlying physical ports' ability to join a LAG, and their administrative state once aggregated.

Syntax

set port lacp port *port-string* {[**aadminkey** *aadminkey*] [**adminstate** {**lacpactive** | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire**}] [**aportpri** *aportpri*] [**asyspri** *asyspri*] [**enable** | [**disable**] [**padminkey** *padminkey*] [**padminport** *padminport*] [**padminportpri** *padminportpri*] [**padminstate** {**lacpactive** | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire**}] [**padminsysid** *padminsysid*] [**padminsyspri** *padminsyspri*]

Parameters

port *port-string*	Specifies the physical port(s) on which to configure LACP. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
aadminkey *aadminkey*	Sets the port's actor admin key. LACP will use this value to form an oper key and will determine which underlying physical ports are capable of aggregating by comparing oper keys. Aggregator ports allow only underlying ports with oper keys matching theirs to join their LAG. Valid values are **1** - **65535**. The default key value is 32768.

aadminstate lacpactive | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire**	Sets the port's actor LACP administrative state to allow for: **lacpactive** - Transmitting LACP PDUs. **lacptimeout** - Transmitting LACP PDUs every 1 sec. vs 30 sec. (default). **lacpagg** - Aggregation on this port. **lacpsync** - Transition to synchronization state. **lacpcollect** - Transition to collection state. **lacpdist** - Transition to distribution state. **lacpdef** - Transition to defaulted state. **lacpexpire** - Transition to expired state.
aportpri *aportpri*	Sets the port's actor port priority. Valid values are **0** - **65535**, with lower values designating higher priority.
asyspri *asyspri*	Sets the port's actor system priority. The LACP implementation on the SecureStack C3 device uses this value to determine aggregation precedence when there are two devices competing for the same aggregator. Valid values are **0** - **65535**, with higher precedence given to lower values.  **Note:** Only one LACP system priority can be set on a SecureStack C3 device, using either this command, or the **set lacp asyspri** command ("set lacp asyspri" on page 7-47).
enable	(Optional) Enables LACPDU processing on this port.
disable	(Optional) Disables LACPDU processing on this port.
padminkey *padminkey*	Sets a default value to use as the port's partner admin key. Only ports with matching admin keys are allowed to aggregate. Valid values are **1** - **65535**.
padminport *padminport*	Sets a default value to use as the port's partner admin value. Valid values are **1** - **65535.**
padminportpri *padminportpri*	Sets a default value to use as the port's partner port priority. Valid values are **0** - **65535**, with lower values given higher priority.
padminstate lacpactive | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire**	Sets a port's partner LACP administrative state. See **aadminstate** for valid options.
padminsysid *padminsysid*	Sets a default value to use as the port's partner system ID. This is a MAC address.
padminsyspri *padminsyspri*	Sets a default value to use as the port's partner priority. Valid values are **0** - **65535**, with lower values given higher priority.

Defaults

At least one parameter must be entered per *port-string*.

If **enable** or **disable** are not specified, port(s) will be enabled with the LACP parameters entered.

Mode

Switch command, read-write.

Usage

LACP commands and parameters beginning with an "a" (such as **aadminkey**) set actor values. Corresponding commands and parameters beginning with a "p" (such as **padminkey**) set corresponding partner values. Actor refers to the local device participating in LACP negotiation, while partner refers to its remote device partner at the other end of the negotiation. Actors and partners maintain current status of the other via LACPDUs containing information about their ports' LACP status and operational state.

Example

This example shows how to set the actor admin key to 3555 for port `ge.3.16`:

```
C3(su)->set port lacp port ge.3.16 aadminkey 3555
```

clear port lacp

Use this command to clear link aggregation settings for one or more ports.

Syntax

```
clear port lacp port port-string {[aadminkey] [aportpri] [asyspri] [aadminstate
{lacpactive | lacptimeout | lacpagg | lacpsync | lacpcollect | lacpdist | lacpdef
| lacpexpire | all}] [padminsyspri] [padminsysid] [padminkey] [padminportpri]
[padminport] [padminstate {lacpactive | lacptimeout | lacpagg | lacpsync |
lacpcollect | lacpdist | lacpdef | lacpexpire | all}]}
```

Parameters

port *port-string*	Specifies the physical port(s) on which LACP settings will be cleared. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
aadminkey	Clears a port's actor admin key.
aportpri	Clears a port's actor port priority.
asyspri	Clears the port's actor system priority.
aadminstate lacpactive | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire** | **all**	Clears a port's specific actor admin state, or all actor admin state(s). For descriptions of specific states, refer to the **set port lacp** command ("set port lacp" on page 7-52).
padminsyspri	Clears the port's default partner priority value.
padminsysid	Clears the port's default partner system ID.
padminkey	Clears the port's default partner admin key.
padminportpri	Clears the port's default partner port priority.

padminport	Deletes a partner port from the LACP configuration.
padminstate lacpactive | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire** | **all**	Clears the port's specific partner admin state, or all partner admin state(s).

Defaults

None.

Mode

Switch command, read-write.

Usage

If you set a port to LACP passive using the command **clear port lacp port** <*port-string*> **aadminstate lacpactive**, the command **clear port lacp port** <*port-string*> **aadminstate lacptimeout** will also be added to the configuration. If you unset the first command, it will remove the second command automatically from the configuration file.

Example

This example shows how to clear all link aggregation parameters for port `ge.3.16`:

```
C3(su)->clear port lacp port ge.3.16
```

Configuring Protected Ports

The Protected Port feature is used to prevent ports from forwarding traffic to each other, even when they are on the same VLAN. Ports may be designated as either protected or unprotected. Ports are unprotected by default. Multiple groups of protected ports are supported.

Protected Port Operation

Ports that are configured to be protected cannot forward traffic to other protected ports in the same group, regardless of having the same VLAN membership. However, protected ports can forward traffic to ports which are unprotected (not listed in any group). Protected ports can also forward traffic to protected ports in a different group, if they are in the same VLAN. Unprotected ports can forward traffic to both protected and unprotected ports. A port may belong to only one group of protected ports.

This feature only applies to ports within a switch or a stack. It does not apply across multiple switches in a network.

Commands

set port protected

Use this command to specify a port to be protected and assign the port to a group of protected ports. A port can be assigned to only one group.

Syntax

`set port protected` *`port-string group-id`*

Parameters

port-string	Specifies the port or ports to be protected.
group-id	Specifies the id of the group to which the ports should be assigned. Id can range from 0 to 2.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to assign ports ge.1.1 through ge.1.3 to protected port group 1:

```
C3(rw)->set port protected ge.1.1-3 1
```

show port protected

Use this command to display information about the ports configured for protected mode.

Syntax

show port protected [*port-string*] | [*group-id*]

Parameters

port-string	(Optional) Specifies the port or ports for which to display information.
group-id	(Optional) Specifies the id of the group for which to display information. Id can range from 0 to 2.

Defaults

If no parameters are entered, information about all protected ports is displayed.

Mode

Read-only.

Example

This example shows how to display information about all protected ports:

```
C3(ro)->show port protected
Group id      Port
----------------------
1             ge.1.1
1             ge.1.2
1             ge.1.3
```

clear port protected

Use this command to remove a port or group from protected mode.

Syntax

clear port protected [*port-string*] | [*group-id*]

Parameters

port-string	(Optional) Specifies the port or ports to remove from protected mode.
group-id	(Optional) Specifies the id of the group to remove from protected mode. Id can range from 0 to 2.

Defaults

If no parameters are entered, all protected ports and groups are cleared.

Mode

Switch command, read-write.

Example

This example shows how to clear protected ports ge.1.1 through ge.1.3:

```
C3(rw)->clear port protected ge.1.1-3
```

set port protected name

Use this command to assign a name to a protected port group id.

Syntax

set port protected name *group-id name*

Parameters

group-id	Specifies the id of this group. Id can range from 0 to 2.
name	Specifies a name for the group. The name can be up to 32 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to assign the name “group1” to protected port group 1:

```
C3(rw)->set port protected name 1 group1
```

show port protected name

Use this command to display the name for the group ids specified.

Syntax

show port protected name *group-id*

Parameters

group-id	Specifies the id of the group to display. Id can range from 0 to 2.

Defaults

None.

Mode

Read-only.

Example

This example shows how to show the name of protected port group 1:

```
C3(ro)->show port protected name 1
Group ID       Group Name
----------------------------
1              group1
```

clear port protected name

Use this command to clear the name of a protected group.

Syntax

clear port protected name *group-id*

Parameters

group-id	Specifies the id of the group for which to clear the name. Id can range from 0 to 2.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the name of protected port group 1:

```
C3(rw)->clear port protected name 1
```

8

SNMP Configuration

This chapter describes the Simple Network Management Protocol (SNMP) set of commands and how to use them.

Note: An Enterasys Networks Feature Guide document containing an in-depth discussion of SNMP configuration is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

SNMP Configuration Summary

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SecureStack C3 devices support three versions of SNMP:

- Version 1 (SNMPv1) — This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of functionality.
- Version 2 (SNMPv2c) — The second release of SNMP, described in RFC 1907, has additions and enhancements to data types, counter size, and protocol operations.
- Version 3 (SNMPv3) — This is the most recent version of SNMP, and includes significant enhancements to administration and security. SNMPv3 is fully described in RFC 2571, RFC 2572, RFC 2573, RFC 2574, and RFC 2575.

SNMPv1 and SNMPv2c

The components of SNMPv1 and SNMPv2c network management fall into three categories:

- Managed devices (such as a switch).
- SNMP agents and MIBs, including SNMP traps, community strings, and Remote Monitoring (RMON) MIBs, which run on managed devices.
- SNMP network management applications, such as the Enterasys NetSight application, which communicate with agents to get statistics and alerts from the managed devices.

SNMPv3

SNMPv3 is an interoperable standards-based protocol that provides secure access to devices by authenticating and encrypting frames over the network. The advanced security features provided in SNMPv3 are as follows:

  - Message integrity — Collects data securely without being tampered with or corrupted.
  - Authentication — Determines the message is from a valid source.
  - Encryption — Scrambles the contents of a frame to prevent it from being seen by an unauthorized source.

Unlike SNMPv1 and SNMPv2c, in SNMPv3, the concept of SNMP agents and SNMP managers no longer apply. These concepts have been combined into an SNMP entity. An SNMP entity consists of an SNMP engine and SNMP applications. An SNMP engine consists of the following four components:

- Dispatcher — This component sends and receives messages.
- Message processing subsystem — This component accepts outgoing PDUs from the dispatcher and prepares them for transmission by wrapping them in a message header and returning them to the dispatcher. The message processing subsystem also accepts incoming messages from the dispatcher, processes each message header, and returns the enclosed PDU to the dispatcher.
- Security subsystem — This component authenticates and encrypts messages.
- Access control subsystem — This component determines which users and which operations are allowed access to managed objects.

About SNMP Security Models and Levels

An SNMP security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. The three levels of SNMP security are: No authentication required (NoAuthNoPriv); authentication required (AuthNoPriv); and privacy (authPriv). A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP frame. Table 8-1 identifies the levels of SNMP security available on SecureStack C3 devices and authentication required within each model.

Table 8-1 SNMP Security Levels

Model	Security Level	Authentication	Encryption	How It Works
v1	NoAuthNoPriv	Community string	None	Uses a community string match for authentication.
v2c	NoAuthNoPriv	Community string	None	Uses a community string match for authentication.
v3	NoAuthNoPriv	User name	None	Uses a user name match for authentication.
	AuthNoPriv	MD5 or SHA	None	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

Using SNMP Contexts to Access Specific MIBs

By default, when operating from the switch CLI, SecureStack C3 devices allow access to all SNMP MIBs or contexts. A context is a collection of MIB objects, often associated with a particular physical or logical device.

If no optional *context* parameters are configured for v1 and v2 "community" names and v3 "user" groups, these groups are able to access all SNMP MIB objects when in switch mode.

Specifying a *context* parameter when setting up SNMP user group would permit or restrict the group's switch management access to the MIB(s) specified by the *context* (MIB object ID) value.

All SNMP contexts known to the device can be displayed using the **show snmp context** command as described in "show snmp context" on page 8-21.

Example

This example permits the "powergroup" to manage all MIBs via SNMPv3:

```
C3(su)->set snmp access powergroup security-model usm
```

Configuration Considerations

Commands for configuring SNMP on the SecureStack C3 device are independent during the SNMP setup process. For instance, target parameters can be specified when setting up optional notification filters — even though these parameters have not yet been created with the **set snmp targetparams** command.

Reviewing SNMP Statistics

Purpose

To review SNMP statistics.

Commands

show snmp engineid

Use this command to display the SNMP local engine ID. This is the SNMP v3 engine's administratively unique identifier.

Syntax

`show snmp engineid`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display SNMP engine properties:

```
C3(su)->show snmp engineid
EngineId: 80:00:15:f8:03:00:e0:63:9d:b5:87
Engine Boots    = 12
Engine Time     = 162181
Max Msg Size    = 2048
```

Table 8-2 provides an explanation of the command output.

Table 8-2 show snmp engineid Output Details

Output Field	What It Displays...
EngineId	String identifying the SNMP agent on the device.
Engine Boots	Number of times the SNMP engine has been started or reinitialized.
Engine Time	Time in seconds since last reboot.
Max Msg Size	Maximum accepted length, in bytes, of SNMP frame.

show snmp counters

Use this command to display SNMP traffic counter values.

Syntax

show snmp counters

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display SNMP counter values

```
C3(su)->show snmp counters

--- mib2 SNMP group counters:
snmpInPkts              = 396601
snmpOutPkts             = 396601
snmpInBadVersions       = 0
snmpInBadCommunityNames = 0
snmpInBadCommunityUses  = 0
snmpInASNParseErrs      = 0
snmpInTooBigs           = 0
snmpInNoSuchNames       = 0
snmpInBadValues         = 0
snmpInReadOnlys         = 0
snmpInGenErrs           = 0
snmpInTotalReqVars      = 403661
snmpInTotalSetVars      = 534
snmpInGetRequests       = 290
snmpInGetNexts          = 396279
snmpInSetRequests       = 32
snmpInGetResponses      = 0
snmpInTraps             = 0
snmpOutTooBigs          = 0
snmpOutNoSuchNames      = 11
snmpOutBadValues        = 0
snmpOutGenErrs          = 0
snmpOutGetRequests      = 0
snmpOutGetNexts         = 0
snmpOutSetRequests      = 0
snmpOutGetResponses     = 396601
snmpOutTraps            = 0
snmpSilentDrops         = 0
snmpProxyDrops          = 0

--- USM Stats counters:
usmStatsUnsupportedSecLevels = 0
usmStatsNotInTimeWindows     = 0
usmStatsUnknownUserNames     = 0
```

```
usmStatsUnknownEngineIDs     = 0
usmStatsWrongDigests         = 0
usmStatsDecryptionErrors     = 0
```

Table 8-3 provides an explanation of the command output.

Table 8-3 show snmp counters Output Details

Output Field	What It Displays...
snmpInPkts	Number of messages delivered to the SNMP entity from the transport service.
snmpOutPkts	Number of SNMP messages passed from the SNMP protocol entity to the transport service.
snmpInBadVersions	Number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
snmpInBadCommunityNames	Number of SNMP messages delivered to the SNMP entity that used an SNMP community name not known to the entity.
snmpInBadCommunityUses	Number of SNMP messages delivered to the SNMP entity that represented an SNMP operation not allowed by the SNMP community named in the message.
snmpInASNParseErrs	Number of ASN.1 (Abstract Syntax Notation) or BER (Basic Encoding Rules) errors encountered by the SNMP entity when decoding received SNMP messages.
snmpInTooBigs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “tooBig.”
snmpInNoSuchNames	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “noSuchName.”
snmpInBadValues	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “badValue.”
snmpInReadOnlys	Number of valid SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as "readOnly."
snmpInGenErrs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as "genErr."
snmpInTotalReqVars	Number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpInTotalSetVars	Number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
snmpInGetRequests	Number of SNMP Get-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetNexts	Number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol entity.
snmpInSetRequests	Number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetResponses	Number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol entity.
snmpInTraps	Number of SNMP Trap PDUs accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as "tooBig."
snmpOutNoSuchNames	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status as "noSuchName."

Table 8-3 show snmp counters Output Details (Continued)

Output Field	What It Displays...
snmpOutBadValues	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as "badValue."
snmpOutGenErrs	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as "genErr."
snmpOutGetRequests	Number of SNMP Get-Request PDUs generated by the SNMP protocol entity.
snmpOutGetNexts	Number of SNMP Get-Next PDUs generated by the SNMP protocol entity.
snmpOutSetRequests	Number of SNMP Set-Request PDUs generated by the SNMP protocol entity.
snmpOutGetResponses	Number of SNMP Get-Response PDUs generated by the SNMP protocol entity.
snmpOutTraps	Number of SNMP Trap PDUs generated by the SNMP protocol entity.
snmpSilentDrops	Number of SNMP Get, Set, or Inform request error messages that were dropped because the reply was larger than the requestor’s maximum message size.
snmpProxyDrops	Number of SNMP Get, Set, or Inform request error messages that were dropped because the reply was larger than the proxy target’s maximum message size.
usmStatsUnsupportedSec Levels	Number of packets received by the SNMP engine that were dropped because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
usmStatsNotInTimeWindows	Number of packets received by the SNMP engine that were dropped because they appeared outside of the authoritative SNMP engine's window.
usmStatsUnknownUserNames	Number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine.
usmStatsUnknownEngineIDs	Number of packets received by the SNMP engine that were dropped because they referenced an snmpEngineID that was not known to the SNMP engine.
usmStatsWrongDigests	Number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value.
usmStatsDecriptionErrors	Number of packets received by the SNMP engine that were dropped because they could not be decrypted.

Configuring SNMP Users, Groups, and Communities

Purpose

To review and configure SNMP users, groups, and v1 and v2 communities. These are defined as follows:

- User — A person registered in SNMPv3 to access SNMP management.
- Group — A collection of users who share the same SNMP access privileges.
- Community — A name used to authenticate SNMPv1 and v2 users.

Commands

show snmp user

Use this command to display information about SNMP users. These are people registered to access SNMP management.

Syntax

show snmp user [**list**] | [*user*] | [**remote** *remote*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

list	(Optional) Displays a list of registered SNMP user names.
user	(Optional) Displays information about a specific user.
remote *remote*	(Optional) Displays information about users on a specific remote SNMP engine.
volatile | **nonvolatile** | **read-only**	(Optional) Displays user information for a specified storage type.

Defaults

If **list** is not specified, detailed SNMP information will be displayed.

If *user* is not specified, information about all SNMP users will be displayed.

If **remote** is not specified, user information about the local SNMP engine will be displayed.

If not specified, user information for all storage types will be displayed.

Mode

Switch command, read-only.

Examples

This example shows how to display an SNMP user list:

```
C3(su)->show snmp user list
--- SNMP user information ---
--- List of registered users:
Guest
admin1
admin2
netops
```

This example shows how to display information for the SNMP "guest" user:

```
(su)->show snmp user guest
--- SNMP user information ---
EngineId:  00:00:00:63:00:00:00:a1:00:00:00:00
Username                = Guest
Auth protocol           = usmNoAuthProtocol
Privacy protocol        = usmNoPrivProtocol
Storage type            = nonVolatile
Row status              = active
```

Table 8-4 provides an explanation of the command output.

Table 8-4 show snmp user Output Details

Output Field	What It Displays...
EngineId	SNMP local engine identifier.
Username	SNMPv1 or v2 community name or SNMPv3 user name.
Auth protocol	Type of authentication protocol applied to this user.
Privacy protocol	Type of encryption protocol applied to this user.
Storage type	Whether entry is stored in **volatile**, **nonvolatile** or **read-only** memory.
Row status	Status of this entry: **active**, **notInService,** or **notReady**.

set snmp user

Use this command to create a new SNMPv3 user.

Syntax

set snmp user *user* [**remote** *remoteid*] [**encryption** {**des** | **aes**}] [**privacy** *privpassword*] [**authentication** {**md5** | **sha**}] [*authpassword*] [**volatile** | **nonvolatile**]

Parameters

user	Specifies a name for the SNMPv3 user.
remote *remoteid*	(Optional) Registers the user on a specific remote SNMP engine.
encryption des | **aes**	(Optional) Specifies the encryption type for this user. AES refers to the Advanced Encryption Standard using a 128 bit key size.
privacy *privpassword*	(Optional) Specifies an encryption password. Minimum of 8 characters. Required if encryption is specified.
authentication md5 | **sha**	(Optional) Specifies the authentication type required for this user as MD5 or SHA.
authpassword	(Optional) Specifies a password for this user when authentication is required. Minimum of 8 characters.
volatile | **nonvolatile**	(Optional) Specifies a storage type for this user entry.

Defaults

If **remote** is not specified, the user will be registered for the local SNMP engine.

If **encryption** is not specified, no encryption will be applied.

If **authentication** is not specified, no authentication will be applied.

If storage type is not specified, **nonvolatile** will be applied.

Mode

Switch command, read-write.

Usage

Although all the parameters except for the user name are optional, if you are entering any of the optional parameters, it is recommended that you enter them in the order shown in the syntax statement.

Examples

This example shows how to create a new SNMP user named “netops”**.** By default, this user will be registered on the local SNMP engine without authentication and encryption. Entries related to this user will be stored in permanent (nonvolatile) memory:

```
C3(su)->set snmp user netops
```

This example creates a new SNMP user named “admin” with DES encryption and MD5 authentication required. The encryption password is “admintest1” and the authentication password is “admintest2.” By default, this user will be registered on the local SNMP engine and entries related to this user will be stored in permanent (nonvolatile) memory.

```
C3(su)->set snmp user admin encryption des privacy admintest1 authentication md5
admintest2
```

clear snmp user

Use this command to remove a user from the SNMPv3 security-model list.

Syntax

clear snmp user *user* [**remote** *remote*]

Parameters

user	Specifies an SNMPv3 user to remove.
remote *remote*	(Optional) Removes the user from a specific remote SNMP engine.

Defaults

If **remote** is not specified, the user will be removed from the local SNMP engine.

Mode

Switch command, read-write.

Example

This example shows how to remove the SNMP user named "bill":

```
C3(su)->clear snmp user bill
```

show snmp group

Use this command to display an SNMP group configuration. An SNMP group is a collection of SNMPv3 users who share the same access privileges.

Syntax

show snmp group [**groupname** *groupname*] [**user** *user*] [**security-model** {**v1** | **v2c** | **usm**}] [**volatile** | **nonvolatile** | **read-only**]

Parameters

groupname *groupname*	(Optional) Displays information for a specific SNMP group.
user *user*	(Optional) Displays information about users within the specified group.
security-model v1 | **v2c** | **usm**	(Optional) Displays information about groups assigned to a specific security SNMP model.
volatile | **nonvolatile** | **read-only**	(Optional) Displays SNMP group information for a specified storage type.

Defaults

If *groupname* is not specified, information about all SNMP groups will be displayed.

If *user* is not specified, information about all SNMP users will be displayed.

If **security-model** is not specified, user information about all SNMP versions will be displayed.

If not specified, information for all storage types will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display SNMP group information:

```
C3(su)->show snmp group
--- SNMP group information ---
Security model          = SNMPv1
Security/user name      = public
Group name              = Anyone
Storage type            = nonVolatile
Row status              = active

Security model          = SNMPv1
Security/user name      = public.router1
Group name              = Anyone
Storage type            = nonVolatile
Row status              = active
```

Table 8-5 provides an explanation of the command output.

Table 8-5 show snmp group Output Details

Output Field	What It Displays...
Security model	SNMP version associated with this group.
Security/user name	User belonging to the SNMP group.
Group name	Name of SNMP group.
Storage type	Whether entry is stored in **volatile**, **nonvolatile** or **read-only** memory.
Row status	Status of this entry: **active**, **notInService,** or **notReady**.

set snmp group

Use this command to create an SNMP group. This associates SNMPv3 users to a group that shares common access privileges.

Syntax

set snmp group *groupname* **user** *user* **security-model** {**v1** | **v2c** | **usm**} [**volatile** | **nonvolatile**]

Parameters

groupname	Specifies an SNMP group name to create.
user *user*	Specifies an SNMPv3 user name to assign to the group.
security-model v1 | **v2c** | **usm**	Specifies an SNMP security model to assign to the group.
volatile | **nonvolatile**	(Optional) Specifies a storage type for SNMP entries associated with the group.

Defaults

If storage type is not specified, **nonvolatile** storage will be applied.

Mode

Switch command, read-write.

Example

This example shows how to create an SNMP group called “anyone”, assign a user named “public” and assign SNMPv3 security to the group:

```
C3(su)->set snmp group anyone user public security-model usm
```

clear snmp group

Use this command to clear SNMP group settings globally or for a specific SNMP group and user.

Syntax

clear snmp group *groupname user* [**security-model** {**v1** | **v2c** | **usm**}]

Parameters

groupname	Specifies the SNMP group to be cleared.
user	Specifies the SNMP user to be cleared.
security-model v1 | **v2c** | **usm**	(Optional) Clears the settings associated with a specific security model.

Defaults

If not specified, settings related to all security models will be cleared.

Mode

Switch command, read-write.

Example

This example shows how to clear all settings assigned to the “public” user within the SNMP group “anyone”:

```
C3(su)->clear snmp group anyone public
```

show snmp community

Use this command to display SNMP community names and status. In SNMPv1 and v2, community names act as passwords to remote management.

Syntax

show snmp community [*name*]

Parameters

name	(Optional) Displays SNMP information for a specific community name.

Defaults

If *name* is not specified, information will be displayed for all SNMP communities.

Mode

Switch command, read-only.

Example

This example shows how to display information about the SNMP "public" community name. For a description of this output, refer to **set snmp community** (page 8-14).

```
C3(su)->show snmp community public

--- Configured community strings ---

Name            = *********
Security name   = public
Context         =
Transport tag   =
Storage type    = nonVolatile
Status          = active
```

set snmp community

Use this command to configure an SNMP community group.

Syntax

set snmp community *community* [**securityname** *securityname*] [**context** *context*] [**transport** *transport*] [**volatile** | **nonvolatile**]

Parameters

community	Specifies a community group name.
securityname *securityname*	(Optional) Specifies an SNMP security name to associate with this community.
context *context*	(Optional) Specifies a subset of management information this community will be allowed to access. Valid values are full or partial context names. To review all contexts configured for the device, use the **show snmp context** command as described in "show snmp context" on page 8-21.
transport *transport*	(Optional) Specifies the set of transport endpoints from which SNMP request with this community name will be accepted. Makes a link to a target address table.
volatile | **nonvolatile**	(Optional) Specifies the storage type for these entries.

Defaults

If **securityname** is not specified, the *community* name will be used.

If **context** is not specified, the default (NULL) context is applied.

If **transport** tag is not specified, none will be applied.

If storage type is not specified, **nonvolatile** will be applied.

Mode

Switch command, read-write.

Usage

When you configure a community name, if you don't specify a context with the **context** parameter, the default (NULL) context is applied. If you want to change a configured context back to the default (NULL)context, enter a hyphen as the value of the **context** parameter, as shown in the Examples below.

Examples

This example shows how to set an SNMP community name called "vip."

```
C3(su)->set snmp community vip
```

The example shows how to set the context for SNMP community "vip" to the default NULL context.

```
C3(su)->set snmp community vip context -
```

clear snmp community

Use this command to delete an SNMP community name.

Syntax

clear snmp community *name*

Parameters

name	Specifies the SNMP community name to clear.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to delete the community name "vip."

```
C3(su)->clear snmp community vip
```

Configuring SNMP Access Rights

Purpose

To review and configure SNMP access rights, assigning viewing privileges and security levels to SNMP user groups.

Commands

show snmp access

Use this command to display access rights and security levels configured for SNMP one or more groups.

Syntax

show snmp access [*groupname*] **[security-model {v1 | v2c | usm}] [noauthentication | authentication | privacy]** [**context** *context*] [**volatile** | **nonvolatile | read-only**]

Parameters

groupname	(Optional) Displays access information for a specific SNMPv3 group.
security-model v1 | **v2c** | **usm**	(Optional) Displays access information for SNMP security model version 1, 2c or 3 (usm).
noauthentication | **authentication** | **privacy**	(Optional) Displays access information for a specific security level.
context *context*	(Optional) Displays access information for a specific context. For a description of how to specify SNMP contexts, refer to "Using SNMP Contexts to Access Specific MIBs" on page 8-3.
volatile | **nonvolatile** | **read-only**	(Optional) Displays access entries for a specific storage type.

Defaults

If *groupname* is not specified, access information for all SNMP groups will be displayed.

If **security-mode**l is not specified, access information for all SNMP versions will be displayed.

If **noauthentication**, **authentication** or **privacy** are not specified, access information for all security levels will be displayed.

If **context** is not specified, all contexts will be displayed.

If **volatile**, **nonvolatile** or **read-only** are not specified, all entries of all storage types will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display SNMP access information:

```
C3(su)->show snmp access
Group           = SystemAdmin
Security model  = USM
Security level  = noAuthNoPriv
Read View       = All
Write View      =
Notify View     = All
Context match   = exact match
Storage type    = nonVolatile
Row status      = active

Group           = NightOperator
Security model  = USM
Security level  = noAuthNoPriv
Read View       = All
Write View      =
Notify View     = All
Context match   = exact match
Storage type    = nonVolatile
Row status      = active
```

Table 8-6 provides an explanation of the command output.

Table 8-6 show snmp access Output Details

Output Field	What It Displays...
Group	SNMP group name.
Security model	Security model applied to this group. Valid types are: **SNMPv1**, **SNMPv2c**, and SNMPv3 (User based - **USM**).
Security level	Security level applied to this group. Valid levels are: • noAuthNoPrivacy (**no authentication** required) • AuthNoPrivacy (**authentication** required) • authPriv (**privacy** -- most secure level)
Read View	Name of the view that allows this group to view SNMP MIB objects.
Write View	Name of the view that allows this group to configure the contents of the SNMP agent**.**
Notify View	Name of the view that allows this group to send an SNMP trap message.
Context match	Whether or not SNMP context match must be exact (full context name match) or a partial match with a given prefix.
Storage type	Whether access entries for this group are stored in **volatile**, **nonvolatile** or **read-only** memory.
Row status	Status of this entry: **active**, **notInService,** or **notReady**.

set snmp access

Use this command to set an SNMP access configuration.

Syntax

```
set snmp access groupname security-model {v1 | v2c | usm} [noauthentication |
authentication | privacy] [context context] [exact | prefix] [read read] [write
write] [notify notify] [volatile | nonvolatile]
```

Parameters

groupname	Specifies a name for an SNMPv3 group.
security-model v1 | v2c | usm	Specifies SNMP version 1, 2c or 3 (usm).
noauthentication | authentication | privacy	(Optional) Applies SNMP security level as no authentication, authentication (without privacy) or privacy. Privacy specifies that messages sent on behalf of the user are protected from disclosure.
context *context* **exact | prefix**	(Optional) Sets the context for this access configuration and specifies that the match must be exact (matching the whole context string) or a prefix match only. Context is a subset of management information this SNMP group will be allowed to access. Valid values are full or partial context names. To review all contexts configured for the device, use the **show snmp context** command as described in "show snmp context" on page 8-21.
read *read*	(Optional) Specifies a read access view.
write *write*	(Optional) Specifies a write access view.
notify *notify*	(Optional) Specifies a notify access view.
volatile | nonvolatile | read-only	(Optional) Stores associated SNMP entries as temporary or permanent, or read-only.

Defaults

If security level is not specified, no authentication will be applied.

If **context** is not specified, access will be enabled for the default context. If **context** is specified without a context match, **exact** match will be applied.

If **read** view is not specified none will be applied.

If **write** view is not specified, none will be applied.

If **notify** view is not specified, none will be applied.

If storage type is not specified, entries will be stored as permanent and will be held through device reboot.

Mode

Switch command, read-write.

Example

This example permits the "powergroup" to manage all MIBs via SNMPv3:

```
C3(su)->set snmp access powergroup security-model usm
```

clear snmp access

Use this command to clear the SNMP access entry of a specific group, including its set SNMP security-model, and level of security.

Syntax

clear snmp access *groupname* **security-model** {**v1** | **v2c** | **usm**} [**noauthentication** | **authentication** | **privacy**] [**context** *context*]

Parameters

groupname	Specifies the name of the SNMP group for which to clear access.
security-model v1 | **v2c** | **usm**	Specifies the security model to be cleared for the SNMP access group.
noauthentication | **authentication** | **privacy**	(Optional) Clears a specific security level for the SNMP access group.
context *context*	(Optional) Clears a specific context for the SNMP access group. Enter / - / to clear the default context.

Defaults

If security level is not specified, all levels will be cleared.

If **context** is not specified, none will be applied.

Mode

Switch command, read-write.

Example

This example shows how to clear SNMP version 3 access for the “mis-group” via the authentication protocol:

```
C3(su)->clear snmp access mis-group security-model usm authentication
```

Configuring SNMP MIB Views

Purpose

To review and configure SNMP MIB views. SNMP views map SNMP objects to access rights.

Commands

For information about...	Refer to page...
show snmp view	8-20
show snmp context	8-21
set snmp view	8-21
clear snmp view	8-22

show snmp view

Use this command to display the MIB configuration for SNMPv3 view-based access (VACM).

Syntax

show snmp view [*viewname*] [**subtree** *oid-or-mibobject*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

viewname	(Optional) Displays information for a specific MIB view.
subtree *oid-or-mibobject*	(Optional) Displays information for a specific MIB subtree when *viewname* is specified.
volatile | **nonvolatile** | **read-only**	(Optional) Displays entries for a specific storage type.

Defaults

If no parameters are specified, all SNMP MIB view configuration information will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display SNMP MIB view configuration information:

```
C3(su)->show snmp view

 --- SNMP MIB View information ---
View Name       = All
Subtree OID     = 1
Subtree mask    =
View Type       = included
Storage type    = nonVolatile
Row status      = active

View Name       = All
Subtree OID     = 0.0
Subtree mask    =
View Type       = included
Storage type    = nonVolatile
Row status      = active

View Name       = Network
Subtree OID     = 1.3.6.1.2.1
Subtree mask    =
View Type       = included
Storage type    = nonVolatile
Row status      = active
```

Table 8-7 provides an explanation of the command output. For details on using the **set snmp view** command to assign variables, refer to “set snmp view” on page 8-21.

Table 8-7 show snmp view Output Details

Output Field	What It Displays...
View Name	Name assigned to a MIB view.
Subtree OID	Name identifying a MIB subtree.
Subtree mask	Bitmask applied to a MIB subtree.
View Type	Whether or not subtree use must be **included** or **excluded** for this view.
Storage type	Whether storage is in **nonVolatile** or **Volatile** memory
Row status	Status of this entry: **active**, **notInService,** or **notReady**.

show snmp context

Use this command to display the context list configuration for SNMP's view-based access control.

Syntax

show snmp context

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Usage

An SNMP context is a collection of management information that can be accessed by an SNMP agent or entity. The default context allows all SNMP agents to access all management information (MIBs). When created using the **set snmp access** command ("set snmp access" on page 8-18), other contexts can be applied to limit access to a subset of management information.

Example

This example shows how to display a list of all SNMP contexts known to the device:

```
C3(su)->show snmp context

--- Configured contexts:
default context (all mibs)
```

set snmp view

Use this command to set a MIB configuration for SNMPv3 view-based access (VACM).

Syntax

set snmp view viewname *viewname* **subtree** *subtree* [**mask** *mask*] [**included** | **excluded**] [**volatile** | **nonvolatile**]

Parameters

viewname *viewname*	Specifies a name for a MIB view.
subtree *subtree*	Specifies a MIB subtree name.
mask *mask*	(Optional) Specifies a bitmask for a subtree.
included | **excluded**	(Optional) Specifies subtree use (default) or no subtree use.
volatile | **nonvolatile**	(Optional) Specifies the use of temporary or permanent (default) storage.

Defaults

If not specified, **mask** will be set to **255.255.255.255**

If not specified, subtree use will be **included**.

If storage type is not specified, **nonvolatile** (permanent) will be applied.

Mode

Switch command, read-write.

Example

This example shows how to set an SNMP MIB view to "public" with a subtree name of 1.3.6.1 included:

```
C3(su)->set snmp view viewname public subtree 1.3.6.1 included
```

clear snmp view

Use this command to delete an SNMPv3 MIB view.

Syntax

clear snmp view *viewname subtree*

Parameters

viewname	Specifies the MIB view name to be deleted.
subtree	Specifies the subtree name of the MIB view to be deleted.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to delete SNMP MIB view "public":

```
C3(su)->clear snmp view public 1.3.6.1
```

Configuring SNMP Target Parameters

Purpose

To review and configure SNMP target parameters. This controls where and under what circumstances SNMP notifications will be sent. A target parameter entry can be bound to a target IP address allowed to receive SNMP notification messages with the **set snmp targetaddr** command ("set snmp targetaddr" on page 8-27).

Commands

For information about...	Refer to page...
show snmp targetparams	8-23
set snmp targetparams	8-24
clear snmp targetparams	8-25

show snmp targetparams

Use this command to display SNMP parameters used to generate a message to a target.

Syntax

show snmp targetparams [*targetParams*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

targetParams	(Optional) Displays entries for a specific target parameter.
volatile | **nonvolatile** | **read-only**	(Optional) Displays target parameter entries for a specific storage type.

Defaults

If *targetParams* is not specified, entries associated with all target parameters will be displayed.

If not specified, entries of all storage types will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display SNMP target parameters information:

```
C3(su)->show snmp targetparams

--- SNMP TargetParams information ---
Target Parameter Name   = v1ExampleParams
Security Name           = public
Message Proc. Model     = SNMPv1
Security Level          = noAuthNoPriv
Storage type            = nonVolatile
Row status              = active
```

```
Target Parameter Name   = v2cExampleParams
Security Name           = public
Message Proc. Model     = SNMPv2c
Security Level          = noAuthNoPriv
Storage type            = nonVolatile
Row status              = active

Target Parameter Name   = v3ExampleParams
Security Name           = CharlieDChief
Message Proc. Model     = USM
Security Level          = authNoPriv
Storage type            = nonVolatile
Row status              = active
```

Table 8-8 provides an explanation of the command output.

Table 8-8 show snmp targetparams Output Details

Output Field	What It Displays...
Target Parameter Name	Unique identifier for the parameter in the SNMP target parameters table. Maximum length is 32 bytes.
Security Name	Security string definition.
Message Proc. Model	SNMP version.
Security Level	Type of security level (**auth**: security level is set to use authentication protocol, **noauth**: security level is not set to use authentication protocol, or **privacy**).
Storage type	Whether entry is stored in **volatile**, **nonvolatile** or **read-only** memory.
Row status	Status of this entry: **active**, **notInService,** or **notReady**.

set snmp targetparams

Use this command to set SNMP target parameters, a named set of security/authorization criteria used to generate a message to a target.

Syntax

set snmp targetparams *paramsname* **user** *user* **security-model** {**v1** | **v2c** | **usm**} **message-processing** {**v1** | **v2c** | **v3**} [**noauthentication** | **authentication** | **privacy**] [**volatile** | **nonvolatile**]

Parameters

paramsname	Specifies a name identifying parameters used to generate SNMP messages to a particular target.
user *user*	Specifies an SNMPv1 or v2 community name or an SNMPv3 user name. Maximum length is 32 bytes.
security-model v1 | **v2c** | **usm**	Specifies the SNMP security model applied to this target parameter as version 1, 2c or 3 (usm).
message-processing v1 | **v2c** | **v3**	Specifies the SNMP message processing model applied to this target parameter as version 1, 2c or 3.

noauthentication | **authentication** | **privacy**	(Optional) Specifies the SNMP security level applied to this target parameter as no authentication, authentication (without privacy) or privacy. Privacy specifies that messages sent on behalf of the user are protected from disclosure.
volatile | **nonvolatile**	(Optional) Specifies the storage type applied to this target parameter.

Defaults

None.

If not specified, security level will be set to **noauthentication.**

If not specified, storage type will be set to **nonvolatile**.

Mode

Switch command, read-write.

Example

This example shows how to set SNMP target parameters named "v1ExampleParams" for a user named "fred" using version 3 security model and message processing, and authentication:

```
C3(su)->set snmp targetparams v1ExampleParams user fred security-model usm
message-processing v3 authentication
```

clear snmp targetparams

Use this command to clear the SNMP target parameter configuration.

Syntax

clear snmp targetparams *targetParams*

Parameters

targetParams	Specifies the name of the parameter in the SNMP target parameters table to be cleared.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear SNMP target parameters named "v1ExampleParams":

```
C3(su)->clear snmp targetparams v1ExampleParams
```

Configuring SNMP Target Addresses

Purpose

To review and configure SNMP target addresses which will receive SNMP notification messages. An address configuration can be linked to optional SNMP transmit, or target, parameters (such as timeout, retry count, and UDP port) set with the **set snmp targetparams** command (page 8-24).

Commands

For information about...	Refer to page...
show snmp targetaddr	8-26
set snmp targetaddr	8-27
clear snmp targetaddr	8-28

show snmp targetaddr

Use this command to display SNMP target address information.

Syntax

show snmp targetaddr [*targetAddr*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

targetAddr	(Optional) Displays information for a specific target address name.
volatile | **nonvolatile** | **read-only**	(Optional) When target address is specified, displays target address information for a specific storage type.

Defaults

If *targetAddr* is not specified, entries for all target address names will be displayed.

If not specified, entries of all storage types will be displayed for a target address.

Mode

Switch command, read-only.

Example

This example shows how to display SNMP target address information:

```
C3(su)->show snmp targetaddr
Target Address Name     = labmachine
Tag List                = v2cTrap
IP Address              = 10.2.3.116
UDP Port#               = 162
Target Mask             = 255.255.255.255
Timeout                 = 1500
Retry count             = 4
Parameters              = v2cParams
Storage type            = nonVolatile
```

```
Row status              = active
```

Table 8-9 provides an explanation of the command output.

Table 8-9 show snmp targetaddr Output Details

Output Field	What It Displays...
Target Address Name	Unique identifier in the snmpTargetAddressTable.
Tag List	Tags a location to the target address as a place to send notifications.
IP Address	Target IP address.
UDP Port#	Number of the UDP port of the target host to use.
Target Mask	Target IP address mask.
Timeout	Timeout setting for the target address.
Retry count	Retry setting for the target address.
Parameters	Entry in the snmpTargetParamsTable.
Storage type	Whether entry is stored in **volatile**, **nonvolatile** or **read-only** memory.
Row status	Status of this entry: **active**, **notInService,** or **notReady**.

set snmp targetaddr

Use this command to configure an SNMP target address. The target address is a unique identifier and a specific IP address that will receive SNMP notification messages and determine which community strings will be accepted. This address configuration can be linked to optional SNMP transmit parameters (such as timeout, retry count, and UDP port).

Syntax

set snmp targetaddr *targetaddr ipaddr* **param** *param* [**udpport** *udpport*] [**mask** *mask*] [**timeout** *timeout*] [**retries** *retries*] [**taglist** *taglist*] [**volatile** | **nonvolatile**]

Parameters

targetaddr	Specifies a unique identifier to index the snmpTargetAddrTable. Maximum length is 32 bytes.
ipaddr	Specifies the IP address of the target.
param *param*	Specifies an entry in the SNMP target parameters table, which is used when generating a message to the target. Maximum length is 32 bytes.
udpport *udpport*	(Optional) Specifies which UDP port of the target host to use.
mask *mask*	(Optional) Specifies the IP mask of the target.
timeout *timeout*	(Optional) Specifies the maximum round trip time allowed to communicate to this target address. This value is in .01 seconds and the default is 1500 (15 seconds.)
retries *retries*	(Optional) Specifies the number of message retries allowed if a response is not received. Default is 3.

taglist *taglist*	(Optional) Specifies a list of SNMP notify tag values. This tags a location to the target address as a place to send notifications. List must be enclosed in quotes and tag values must be separated by a space (for example, **"tag 1 tag 2"**).
volatile | **nonvolatile**	(Optional) Specifies temporary (default), or permanent storage for SNMP entries.

Defaults

If not specified, *udpport* will be set to **162**.

If not specified, *mask* will be set to **255.255.255.255**

If not specified, *timeout* will be set to **1500**.

If not specified, number of *retries* will be set to **3**.

If **taglist** is not specified, none will be set.

If not specified, storage type will be **nonvolatile**.

Mode

Switch command, read-write.

Example

This example shows how to configure a trap notification called "**TrapSink."** This trap notification will be sent to the workstation 192.168.190.80 (which is target address "tr"). It will use security and authorization criteria contained in a target parameters entry called "v2cExampleParams". For more information on configuring a basic SNMP trap, refer to "Creating a Basic SNMP Trap Configuration" on page 8-37:

```
C3(su)->set snmp targetaddr tr 192.168.190.80 param v2cExampleParams taglist
TrapSink
```

clear snmp targetaddr

Use this command to delete an SNMP target address entry.

Syntax

`clear snmp targetaddr` *`targetAddr`*

Parameters

targetAddr	Specifies the target address entry to delete.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear SNMP target address entry “tr”:

```
C3(su)->clear snmp targetaddr tr
```

Configuring SNMP Notification Parameters

About SNMP Notify Filters

Profiles indicating which targets should not receive SNMP notification messages are kept in the NotifyFilter table. If this table is empty, meaning that no filtering is associated with any SNMP target, then no filtering will take place. “Traps” or “informs” notifications will be sent to all destinations in the SNMP targetAddrTable that have tags matching those found in the NotifyTable.

When the NotifyFilter table contains profile entries, the SNMP agent will find any filter profile name that corresponds to the target parameter name contained in an outgoing notification message. It will then apply the appropriate subtree-specific filter when generating notification messages.

Purpose

To configure SNMP notification parameters and optional filters. Notifications are entities which handle the generation of SNMP v1 and v2 “traps” or SNMP v3 “informs” messages to select management targets. Optional notification filters identify which targets should not receive notifications. For a sample SNMP trap configuration showing how SNMP notification parameters are associated with security and authorization criteria (target parameters) and mapped to a management target address, refer to “Creating a Basic SNMP Trap Configuration” on page 8-37.

Commands

For information about...	Refer to page...
show newaddrtrap	8-30
set newaddrtrap	8-30
show snmp notify	8-31
set snmp notify	8-32
clear snmp notify	8-33
show snmp notifyfilter	8-33
set snmp notifyfilter	8-34
clear snmp notifyfilter	8-35
show snmp notifyprofile	8-36
set snmp notifyprofile	8-36
clear snmp notifyprofile	8-37

show newaddrtrap

Use this command to display the global and port-specific status of the SNMP new MAC addresses trap function.

Syntax

show newaddrtrap [*port-string*]

Parameters

port-string	(Optional) Displays the status of the new MAC addresses trap function on specific ports.

Defaults

If *port-string* is not specified, the status of the new MAC addresses trap function will be displayed for all ports.

Mode

Switch command, read-only.

Usage

By default, this function is disabled globally and per port.

Example

This example displays the New Address Trap state for Gigabit Ethernet ports 1 through 5 in unit/slot 1.

```
C3(ro)->show newaddrtrap ge.1.1-5
New Address Traps Globally disabled

Port      Enable State
--------- ------------
ge.1.1    disabled
ge.1.2    disabled
ge.1.3    disabled
ge.1.4    disabled
ge.1.5    disabled
```

set newaddrtrap

Use this command to enable or disable SNMP trap messaging, globally or on one or more ports, when new source MAC addresses are detected.

Syntax

set newaddrtrap [*port-string*] {**enable** | **disable**}

Parameters

port-string	(Optional) Enable or disable the new MAC addresses trap function on specific ports.
enable | **disable**	Enable or disable the new MAC addresses trap function. If entered without the *port-string* parameter, enables or disables the function globally. When entered with the *port-string* parameter, enables or disables the function on specific ports.

Defaults

If *port-string* is not specified, the trap function is set globally.

Mode

Switch mode, read-write.

Usage

This command enables and disables sending SNMP trap messages when a new source MAC address is detected by a port. If the port is a CDP port, however, traps for new source MAC addresses will not be sent.

The default mode is disabled globally and per port.

Example

This example enables the trap function globally and then on Gigabit Ethernet ports 1 through 5 in unit/slot 1.

```
C3(rw)->set newaddrtrap enable
C3(rw)->set newaddrtrap ge.1.1-5 enable
```

show snmp notify

Use this command to display the SNMP notify configuration, which determines the management targets that will receive SNMP notifications.

Syntax

show snmp notify [*notify*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

notify	(Optional) Displays notify entries for a specific notify name.
volatile | **nonvolatile** | **read-only**	(Optional) Displays notify entries for a specific storage type.

Defaults

If a *notify* name is not specified, all entries will be displayed.

If **volatile**, **nonvolatile**, or **read-only** are not specified, all storage type entries will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display the SNMP notify information:

```
C3(su)->show snmp notify

 --- SNMP notifyTable information ---
Notify name     = 1
Notify Tag      = Console
Notify Type     = trap
Storage type    = nonVolatile
Row status      = active

Notify name     = 2
Notify Tag      = TrapSink
Notify Type     = trap
Storage type    = nonVolatile
Row status      = active
```

Table 8-10 provides an explanation of the command output.

Table 8-10 show snmp notify Output Details

Output Field	What It Displays...
Notify name	A unique identifier used to index the SNMP notify table.
Notify Tag	Name of the entry in the SNMP notify table.
Notify Type	Type of notification: SNMPv1 or v2 **trap** or SNMPv3 **InformRequest** message.
Storage type	Whether access entry is stored in **volatile**, **nonvolatile**, or **read-only** memory.
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

set snmp notify

Use this command to set the SNMP notify configuration. This creates an entry in the SNMP notify table, which is used to select management targets who should receive notification messages. This command's **tag** parameter can be used to bind each entry to a target address using the **set snmp targetaddr** command ("set snmp targetaddr" on page 8-27).

Syntax

set snmp notify *notify* **tag** *tag* [**trap** | **inform**] [**volatile** | **nonvolatile**]

Parameters

notify	Specifies an SNMP notify name.
tag *tag*	Specifies an SNMP notify tag. This binds the notify name to the SNMP target address table.
trap | **inform**	(Optional) Specifies SNMPv1 or v2 Trap messages (default) or SNMP v3 InformRequest messages.
volatile | **nonvolatile**	(Optional) Specifies temporary (default), or permanent storage for SNMP entries.

Defaults

If not specified, message type will be set to **trap**.

If not specified, storage type will be set to **nonvolatile**.

Mode

Switch command, read-write.

Example

This example shows how to set an SNMP notify configuration with a notify name of "hello" and a notify tag of "world". Notifications will be sent as trap messages and storage type will automatically default to permanent:

```
C3(su)->set snmp notify hello tag world trap
```

clear snmp notify

Use this command to clear an SNMP notify configuration.

Syntax

clear snmp notify *notify*

Parameters

notify	Specifies an SNMP notify name to clear.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the SNMP notify configuration for "hello":

```
C3(su)->clear snmp notify hello
```

show snmp notifyfilter

Use this command to display SNMP notify filter information, identifying which profiles will not receive SNMP notifications.

Syntax

show snmp notifyfilter [*profile*] [**subtree** *oid-or-mibobject*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

profile	(Optional) Displays a specific notify filter.
subtree *oid-or-mibobject*	(Optional) Displays a notify filter within a specific subtree.
volatile | **nonvolatile** | **read-only**	(Optional) Displays notify filter entries of a specific storage type.

Defaults

If no parameters are specified, all notify filter information will be displayed.

Mode

Switch command, read-only.

Usage

See "About SNMP Notify Filters" on page 8-29 for more information about notify filters.

Example

This example shows how to display SNMP notify filter information. In this case, the notify profile "pilot1" in subtree 1.3.6 will not receive SNMP notification messages:

```
C3(su)->show snmp notifyfilter

--- SNMP notifyFilter information ---
Profile         = pilot1
Subtree         = 1.3.6
Filter type     = included
Storage type    = nonVolatile
Row status      = active
```

set snmp notifyfilter

Use this command to create an SNMP notify filter configuration. This identifies which management targets should NOT receive notification messages, which is useful for fine-tuning the amount of SNMP traffic generated.

Syntax

set snmp notifyfilter *profile* **subtree** *oid-or-mibobject* [**mask** *mask*] [**included** | **excluded**] [**volatile** | **nonvolatile**]

Parameters

profile	Specifies an SNMP filter notify name.
subtree *oid-or-mibobject*	Specifies a MIB subtree ID target for the filter.
mask *mask*	(Optional) Applies a subtree mask.

included | **excluded**	(Optional) Specifies that subtree is included or excluded.
volatile | **nonvolatile**	(Optional) Specifies a storage type.

Defaults

If not specified, **mask** is not set.

If not specified, subtree will be **included**.

If storage type is not specified, **nonvolatile** (permanent) will be applied.

Mode

Switch command, read-write.

Usage

See "About SNMP Notify Filters" on page 8-29 for more information about notify filters.

Example

This example shows how to create an SNMP notify filter called "pilot1" with a MIB subtree ID of 1.3.6:

```
C3(su)->set snmp notifyfilter pilot1 subtree 1.3.6
```

clear snmp notifyfilter

Use this command to delete an SNMP notify filter configuration.

Syntax

`clear snmp notifyfilter` *`profile`* **`subtree`** *`oid-or-mibobject`*

Parameters

profile	Specifies an SNMP filter notify name to delete.
subtree *oid-or-mibobject*	Specifies a MIB subtree ID containing the filter to be deleted.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to delete the SNMP notify filter "pilot1":

```
C3(su)->clear snmp notifyfilter pilot1 subtree 1.3.6
```

show snmp notifyprofile

Use this command to display SNMP notify profile information. This associates target parameters to an SNMP notify filter to determine who should not receive SNMP notifications.

Syntax

show snmp notifyprofile [*profile*] [**targetparam** *targetparam]* [**volatile** | **nonvolatile** | **read-only**]

Parameters

profile	(Optional) Displays a specific notify profile.
targetparam *targetparam*	(Optional) Displays entries for a specific target parameter.
volatile | **nonvolatile** | **read-only**	(Optional) Displays notify filter entries of a specific storage type.

Defaults

If no parameters are specified, all notify profile information will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display SNMP notify information for the profile named "area51":

```
C3(su)->show snmp notifyprofile area51

 --- SNMP notifyProfile information ---
Notify Profile  = area51
TargetParam     = v3ExampleParams
Storage type    = nonVolatile
Row status      = active
```

set snmp notifyprofile

Use this command to create an SNMP notify filter profile configuration. This associates a notification filter, created with the **set snmp notifyfilter** command ("set snmp notifyfilter" on page 8-34), to a set of SNMP target parameters to determine which management targets should not receive SNMP notifications.

Syntax

set snmp notifyprofile *profile* **targetparam** *targetparam* [**volatile** | **nonvolatile**]

Parameters

profile	Specifies an SNMP filter notify name.
targetparam *targetparam*	Specifies an associated entry in the SNMP Target Params Table.
volatile | **nonvolatile**	(Optional) Specifies a storage type.

Defaults

If storage type is not specified, **nonvolatile** (permanent) will be applied.

Mode

Switch command, read-write.

Example

This example shows how to create an SNMP notify profile named area51 and associate a target parameters entry.

```
C3(su)->set snmp notifyprofile area51 targetparam v3ExampleParams
```

clear snmp notifyprofile

Use this command to delete an SNMP notify profile configuration.

Syntax

clear snmp notifyprofile *profile* **targetparam** *targetparam*

Parameters

profile	Specifies an SNMP filter notify name to delete.
targetparam *targetparam*	Specifies an associated entry in the snmpTargetParamsTable.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to delete SNMP notify profile “area51”:

```
C3(su)->clear snmp notifyprofile area51 targetparam v3ExampleParams
```

Creating a Basic SNMP Trap Configuration

Traps are notification messages sent by an SNMPv1 or v2 agent to a network management station, a console, or a terminal to indicate the occurrence of a significant event, such as when a port or device goes up or down, when there are authentication failures, and when power supply errors

occur. The following configuration example shows how to use CLI commands to associate SNMP notification parameters with security and authorization criteria (target parameters), and map the parameters to a management target address.

Note: This example illustrates how to configure an SNMPv2 trap notification. Creating an SNMPv1 or v3 Trap, or an SNMPv3 Inform notification would require using the same commands with different parameters, where appropriate. Always ensure that v1/v2 communities or v3 users used for generating traps or informs are pre-configured with enough privileges to access corresponding MIBs.

Complete an SNMPv2 trap configuration on a SecureStack C3 device as follows:

1. Create a community name that will act as an SNMP user password.
2. Create an SNMP target parameters entry to associate security and authorization criteria to the users in the community created in Step 1.
3. Verify if any applicable SNMP notification entries exist, or create a new one. You will use this entry to send SNMP notification messages to the appropriate management targets created in Step 2.
4. Create a target address entry to bind a management IP address to:
   - The notification entry and tag name created in Step 3 and
   - The target parameters entry created in Step 2.

Table 8-11 shows the commands used to complete an SNMPv2 trap configuration on a SecureStack C3 device.

Table 8-11 Basic SNMP Trap Configuration

To do this...	Use these commands...
Create a community name.	set snmp community
Create an SNMP target parameters entry.	set snmp targetparams
Verify if any applicable SNMP notification entries exist.	show snmp notify
Create a new notification entry.	set snmp notify
Create a target address entry.	set snmp targetaddr

Example

This example shows how to:

- Create an SNMP community called **mgmt**.
- Configure a trap notification called **TrapSink**.

This trap notification will be sent with the community name **mgmt** to the workstation **192.168.190.80** (which is target address **tr**). It will use security and authorization criteria contained in a target parameters entry called **v2cExampleParams**.

```
C3(su)->set snmp community mgmt
C3(su)->set snmp targetparams v2cExampleParams user mgmt
security-model v2c message-processing v2c
C3(su)->set snmp notify entry1 tag TrapSink
C3(su)->set snmp targetaddr tr 192.168.190.80 param v2cExampleParams taglist
TrapSink
```

How SNMP Will Use This Configuration

In order to send a trap/notification requested by a MIB code, the SNMP agent requires the equivalent of a trap "door", a "key" to unlock the door, and a "procedure" for crossing the doorstep. To determine if all these elements are in place, the SNMP agent proceeds as follows:

1. Determines if the "keys" for trap "doors" do exist. In the example configuration above, the key that SNMP is looking for is the notification entry created with the **set snmp notify** command which, in this case, is a key labeled **entry1**.
2. Searches for the doors matching such a key. For example, the parameters set for the **entry1** key shows that it opens only the door **TrapSink**.
3. Verifies that the specified door **TrapSink** is, in fact, available. In this case it was built using the **set snmp targetaddr** command. This command also specifies that this door leads to the management station **192.168.190.80**, and the "procedure" (**targetparams**) to cross the doorstep is called **v2ExampleParams**.
4. Verifies that the **v2ExampleParams** description of how to step through the door is, in fact, there. The agent checks **targetparams** entries and determines this description was made with the **set snmp targetparams** command, which tells exactly which SNMP protocol to use and what community name to provide. In this case, the community name is **mgmt**.
5. Verifies that the **mgmt** community name is available. In this case, it has been configured using the **set snmp community** command.
6. Sends the trap notification message.

Configuring the SNMP Management Interface

Purpose

To configure the source IP address used by the SNMP agent when generating SNMP traps.

Commands

show snmp interface

Use this command to display the interface used for the source IP address of the SNMP agent when generating SNMP traps.

Syntax

```
show snmp interface
```

Parameters

None.

Defaults

None.

Mode

Switch mode, read-only.

Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the SNMP agent.

```
C3(rw)->show snmp interface
loopback 1  192.168.10.1
```

set snmp interface

Use this command to specify the interface used for the source IP address of the SNMP agent when generating SNMP traps.

Syntax

set snmp interface {**loopback** *loop-ID* | **vlan** *vlan-ID*}

Parameters

loopback *loop-ID*	Specifies the loopback interface to be used. The value of *loop-ID* can range from 0 to 7.
vlan *vlan-ID*	Specifies the VLAN interface to be used. The value of vlan-ID can range from 1 to 4093.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command allows you to configure the source IP address used by the SNMP agent when generating SNMP traps. Any of the management interfaces, including VLAN routing interfaces, can be configured as the source IP address used in packets generated by the SNMP agent.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the IP address of the Host interface will be used.

If a non-loopback interface is configured with this command, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the SNMP agent source IP address.

```
C3(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
C3(rw)->router(Config-if(Vlan 100))#exit
C3(rw)->router(Config)#exit
C3(rw)->router#exit
C3(rw)->router>exit
C3(rw)->set snmp interface vlan 100

C3(rw)->show snmp interface
vlan 100  192.168.10.1
```

clear snmp interface

Use this command to clear the interface used for the source IP address of the SNMP agent back to the default of the Host interface.

Syntax

`clear snmp interface`

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This command returns the interface used for the source IP address of the SNMP agent back to the default of the Host interface.

```
C3(rw)->show snmp interface
vlan 100  192.168.10.1
C3(rw)->clear snmp interface
C3(rw)->
```

9

Spanning Tree Configuration

This chapter describes the Spanning Tree Configuration set of commands and how to use them.

Caution: Spanning Tree configuration should be performed only by personnel who are very knowledgeable about Spanning Trees and the configuration of the Spanning Tree Algorithm. Otherwise, the proper operation of the network could be at risk.

Spanning Tree Configuration Summary

Note: An Enterasys Networks Feature Guide document containing an in-depth discussion of Spanning Tree configuration is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

Overview: Single, Rapid, and Multiple Spanning Tree Protocols

The IEEE 802.1D Spanning Tree Protocol (STP) resolves the problems of physical loops in a network by establishing one primary path between any two devices in a network. Any duplicate paths are barred from use and become standby or blocked paths until the original path fails, at which point they can be brought into service.

RSTP

The IEEE 802.1w Rapid Spanning Protocol (RSTP), an evolution of 802.1D, can achieve much faster convergence than legacy STP in a properly configured network. RSTP significantly reduces the time to reconfigure the network's active topology when physical topology or configuration parameter changes occur. It selects one switch as the root of a Spanning Tree-connected active topology and assigns port roles to individual ports on the switch, depending on whether that port is part of the active topology.

RSTP provides rapid connectivity following the failure of a switch, switch port, or a LAN. A new root port and the designated port on the other side of the bridge transition to forwarding through an explicit handshake between them. By default, user ports are configured to rapidly transition to forwarding in RSTP.

MSTP

The IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) builds upon 802.1D and RSTP by optimizing utilization of redundant links between switches in a network. When redundant links exist between a pair of switches running single STP, one link is forwarding while the others are blocking for all traffic flowing between the two switches. The blocking links are effectively used only if the forwarding link goes down. MSTP assigns each VLAN present on the network to a particular Spanning Tree instance, allowing each switch port to be in a distinct state for each such instance: blocking for one Spanning Tree while forwarding for another. Thus, traffic associated with one set of VLANs can traverse a particular inter-switch link, while traffic associated with another set of VLANs can be blocked on that link. If VLANs are assigned to Spanning Trees wisely, no inter-switch link will be completely idle, maximizing network utilization.

For details on creating Spanning Tree instances, refer to “set spantree msti” on page 9-12.

For details on mapping Spanning Tree instances to VLANs, refer to “set spantree mstmap” on page 9-14.

Note: MSTP and RSTP are fully compatible and interoperable with each other and with legacy STP 802.1D.

Spanning Tree Features

The SecureStack C3 device meets the requirements of the Spanning Tree Protocols by performing the following functions:

- Creating a single Spanning Tree from any arrangement of switching or bridging elements.
- Compensating automatically for the failure, removal, or addition of any device in an active data path.
- Achieving port changes in short time intervals, which establishes a stable active topology quickly with minimal network disturbance.
- Using a minimum amount of communications bandwidth to accomplish the operation of the Spanning Tree Protocol.
- Reconfiguring the active topology in a manner that is transparent to stations transmitting and receiving data packets.
- Managing the topology in a consistent and reproducible manner through the use of Spanning Tree Protocol parameters.

Note: The term “bridge” is used as an equivalent to the term “switch” or “device” in this document.

Loop Protect

The Loop Protect feature prevents or short circuits loop formation in a network with redundant paths by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point-to-point inter-switch links (ISLs) before their states are allowed to become forwarding. Further, if a BPDU timeout occurs on a port, its state becomes listening until a BPDU is received.

Both upstream and downstream facing ports are protected. When a root or alternate port loses its path to the root bridge due to a message age expiration it takes on the role of designated port. It will not forward traffic until a BPDU is received. When a port is intended to be the designated port in an ISL it constantly proposes and will not forward until a BPDU is received, and will revert to

listening if it fails to get a response. This protects against misconfiguration and protocol failure by the connected bridge.

The Disputed BPDU mechanism protects against looping in situations where there is one way communication. A disputed BPDU is one in which the flags field indicates a designated role and learning and the priority vector is worse than that already held by the port. If a disputed BPDU is received, the port is forced to the listening state. When an inferior designated BPDU with the learning bit set is received on a designated port, its state is set to discarding to prevent loop formation. Note that the Dispute mechanism is always active regardless of the configuration setting of Loop Protection.

Loop Protect operates as a per port, per MST instance feature. It should be set on inter-switch links. It is comprised of several related functions:

- Control of port forwarding state based on reception of agreement BPDUs
- Control of port forwarding state based on reception of disputed BPDUs
- Communicating port non-forwarding status through traps and syslog messages
- Disabling a port based on frequency of failure events

Port forwarding state in the designated port is gated by a timer that is set upon BPDU reception. It is analogous to the rcvdInfoWhile timer the port uses when receiving root information in the root/alternate/backup role.

There are two operational modes for Loop Protect on a port. If the port is connected to a device known to implement Loop Protect, it uses full functional mode. Otherwise the port operates in limited functional mode.

Connection to a Loop Protect switch guarantees that the alternate agreement mechanism is implemented. This means the designated port can rely on receiving a response to its proposal regardless of the role of the connected port, which has two important implications. First, the designated port connected to a non-root port may transition to forwarding. Second, there is no ambiguity when a timeout happens; a Loop Protect event has occurred.

In full functional mode, when a type 2 BPDU is received and the port is designated and point-to-point, the timer is set to 3 times helloTime. In limited functional mode there is the additional requirement that the flags field indicate a root role. If the port is a boundary port the MSTIs for that port follow the CIST, that is, the MSTI port timers are set according to the CIST port timer. If the port is internal to the region then the MSTI port timers are set independently using the particular MSTI message.

Message age expiration and the expiration of the Loop Protect timer are both Loop Protect events. A notice level syslog message is produced for each such event. Traps may be configured to report these events as well. A syslog message and trap may be configured for disputed BPDUs.

It is also configurable to force the locking of a SID/port for the occurrence of one or more events. When the configured number of events happen within a given window of time, the port is forced into blocking and held there until it is manually unlocked via management.

Configuring Spanning Tree Bridge Parameters

Purpose

To display and set Spanning Tree bridge parameters, including device priorities, hello time, maximum wait time, forward delay, path cost, and topology change trap suppression.

Commands

show spantree stats

Use this command to display Spanning Tree information for one or more ports.

Syntax

show spantree stats [**port** *port-string*] [**sid** *sid*] [**active**]

Parameters

port *port-string*	(Optional) Displays information for the specified port(s). For a detailed description of possible *port--string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
sid sid	(Optional) Displays information for a specific Spanning Tree identifier. If not specified, SID 0 is assumed.
active	(Optional) Displays information for ports that have received STP BPDUs since boot.

Defaults

If *port-string* is not specified, Spanning Tree information for all ports will be displayed.

If *sid* is not specified, information for Spanning Tree 0 will be displayed.

If **active** is not specified information for all ports will be displayed regardless of whether or not they have received BPDUs.

Mode

Switch command, read-only.

Example

This example shows how to display the device's Spanning Tree configuration:

```
C3(su)->show spantree stats

Spanning tree status         - enabled
Spanning tree instance       - 0
Designated Root MacAddr      - 00-e0-63-9d-c1-c8
Designated Root Priority     - 0
Designated Root Cost         - 10000
Designated Root Port         - lag.0.1
Root Max Age                 - 20 sec
Root Hello Time              - 2  sec
Root Forward Delay           - 15 sec
Bridge ID MAC Address        - 00-01-f4-da-5e-3d
Bridge ID Priority           - 32768
Bridge Max Age               - 20 sec
Bridge Hello Time            - 2  sec
Bridge Forward Delay         - 15 sec
Topology Change Count        - 7
Time Since Top Change        - 00 days 03:19:15
Max Hops                     - 20
```

Table 9-1 shows a detailed explanation of command output.

Table 9-1 show spantree Output Details

Output	What It Displays...
Spanning tree instance	Spanning Tree ID.
Spanning tree status	Whether Spanning Tree is enabled or disabled.
Designated Root MacAddr	MAC address of the designated Spanning Tree root bridge.
Designated Root Port	Port through which the root bridge can be reached.
Designated Root Priority	Priority of the designated root bridge.
Designated Root Cost	Total path cost to reach the root.
Root Max Age	Amount of time (in seconds) a BPDU packet should be considered valid.
Root Hello Time	Interval (in seconds) at which the root device sends BPDU (Bridge Protocol Data Unit) packets.
Root Forward Delay	Amount of time (in seconds) the root device spends in listening or learning mode.
Bridge ID MAC Address	Unique bridge MAC address, recognized by all bridges in the network.
Bridge ID Priority	Bridge priority, which is a default value, or is assigned using the **set spantree priority** command. For details, refer to "set spantree priority" on page 9-17.
Bridge Max Age	Maximum time (in seconds) the bridge can wait without receiving a configuration message (bridge "hello") before attempting to reconfigure. This is a default value, or is assigned using the **set spantree maxage** command. For details, refer to "set spantree maxage" on page 9-19.

Table 9-1 show spantree Output Details (Continued)

Output	What It Displays...
Bridge Hello Time	Amount of time (in seconds) the bridge sends BPDUs. This is a default value, or is assigned using the **set spantree hello** command. For details, refer to "set spantree hello" on page 9-18.
Bridge Forward Delay	Amount of time (in seconds) the bridge spends in listening or learning mode. This is a default value, or is assigned using the **set spantree fwddelay** command. For details, refer to "set spantree fwddelay" on page 9-20.
Topology Change Count	Number of times topology has changed on the bridge.
Time Since Top Change	Amount of time (in days, hours, minutes and seconds) since the last topology change.
Max Hops	Maximum number of hops information for a particular Spanning Tree instance may traverse (via relay of BPDUs within the applicable MST region) before being discarded.

set spantree

Use this command to globally enable or disable the Spanning Tree protocol on the switch.

Syntax

```
set spantree {disable | enable}
```

Parameters

disable | **enable**	Globally disables or enables Spanning Tree.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to disable Spanning Tree on the device:

```
C3(su)->set spantree disable
```

show spantree version

Use this command to display the current version of the Spanning Tree protocol running on the device.

Syntax

```
show spantree version
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display Spanning Tree version information for the device:

```
C3(su)->show spantree version
Force Version is mstp
```

set spantree version

Use this command to set the version of the Spanning Tree protocol to MSTP (Multiple Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) or to STP 802.1D-compatible.

Syntax

`set spantree version` {**`mstp`** | **`stpcompatible`** | **`rstp`**}

Parameters

mstp	Sets the version to STP 802.1s-compatible.
stpcompatible	Sets the version to STP 802.1D-compatible.
rstp	Sets the version to 802.1w-compatible.

Defaults

None.

Mode

Switch command, read-write.

Usage

In most networks, Spanning Tree version should not be changed from its default setting of **mstp** (Multiple Spanning Tree Protocol) mode. MSTP mode is fully compatible and interoperable with legacy STP 802.1D and Rapid Spanning Tree (RSTP) bridges. Setting the version to **stpcompatible** mode will cause the bridge to transmit only 802.1D BPDUs, and will prevent non-edge ports from rapidly transitioning to forwarding state.

Example

This example shows how to globally change the Spanning Tree version from the default of MSTP to RSTP:

```
C3(su)->set spantree version rstp
```

clear spantree version

Use this command to reset the Spanning Tree version to MSTP mode.

Syntax

```
clear spantree version
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the Spanning Tree version:

```
C3(su)->clear spantree version
```

show spantree bpdu-forwarding

Use this command to display the Spanning Tree BPDU forwarding mode.

Syntax

```
show spantree bpdu-forwarding
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the Spanning Tree BPDU forwarding mode:

```
C3(su)->show spantree bpdu-forwarding
BPDU forwarding is disabled.
```

set spantree bpdu-forwarding

Use this command to enable or disable Spanning Tree BPDU forwarding. By default BPDU forwarding is disabled.

Syntax

```
set spantree bpdu-forwarding {disable | enable}
```

Parameters

disable | **enable**	Disables or enables BPDU forwarding;.

Defaults

By default BPDU forwarding is disabled.

Mode

Switch command, read-write.

Usage

The Spanning Tree protocol must be disabled (set spantree **disable**) for this feature to take effect.

Example

This example shows how to enable BPDU forwarding:

```
C3(rw)-> set spantree bpdu-forwarding enable
```

show spantree bridgeprioritymode

Use this command to display the Spanning Tree bridge priority mode setting.

Syntax

```
show spantree bridgeprioritymode
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the Spanning Tree bridge priority mode setting:

```
C3(rw)->show spantree bridgeprioritymode
Bridge Priority Mode is set to IEEE802.1t mode.
```

set spantree bridgeprioritymode

Use this command to set the Spanning Tree bridge priority mode to 802.1D (legacy) or 802.1t.

Syntax

```
set spantree bridgeprioritymode {8021d | 8021t}
```

Parameters

8021d	Sets the bridge priority mode to use 802.1D (legacy) values, which are 0 - 65535.
8021t	Sets the bridge priority mode to use 802.1t values, which are 0 to 61440, in increments of 4096. Values will automatically be rounded up or down, depending on the 802.1t value to which the entered value is closest. This is the default bridge priority mode.

Defaults

None

Mode

Switch command, read-write.

Usage

The mode affects the range of priority values used to determine which device is selected as the Spanning Tree root as described in **set spantree priority** ("set spantree priority" on page 9-17). The default for the switch is to use 802.1t bridge priority mode.

Example

This example shows how to set the bridge priority mode to 802.1D:

```
C3(rw)->set spantree bridgeprioritymode 8021d
```

clear spantree bridgeprioritymode

Use this command to reset the Spanning Tree bridge priority mode to the default setting of 802.1t.

Syntax

```
clear spantree bridgeprioritymode
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the bridge priority mode to 802.1t:

```
C3(rw)->clear spantree bridgeprioritymode
```

show spantree mstilist

Use this command to display a list of Multiple Spanning Tree (MST) instances configured on the device.

Syntax

show spantree mstilist

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display a list of MST instances. In this case, SID 2 has been configured:

```
C3(su)->show spantree mstilist
 Configured Multiple Spanning Tree instances:
  2
```

set spantree msti

Use this command to create or delete a Multiple Spanning Tree instance.

Syntax

set spantree msti sid *sid* {**create | delete**}

Parameters

sid *sid*	Sets the Multiple Spanning Tree ID. Valid values are **1** - **4094**. SecureStack C3 devices will support up to 4 MST instances.
create | **delete**	Creates or deletes an MST instance.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to create an MST instance 2:

```
C3(su)->set spantree msti sid 2 create
```

clear spantree msti

Use this command to delete one or more Multiple Spanning Tree instances.

Syntax

clear spantree msti [**sid** *sid*]

Parameters

sid *sid*	(Optional) Deletes a specific multiple Spanning Tree ID.

Defaults

If *sid* is not specified, all MST instances will be cleared.

Mode

Switch command, read-write.

Example

This example shows how to delete all MST instances:

```
C3(su)->clear spantree msti
```

show spantree mstmap

Use this command to display the mapping of a filtering database ID (FID) to a Spanning Trees. Since VLANs are mapped to FIDs, this shows to which SID a VLAN is mapped.

Syntax

show spantree mstmap [**fid** *fid*]

Parameters

fid *fid*	(Optional) Displays information for specific FIDs.

Defaults

If *fid* is not specified, information for all assigned FIDs will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display SID to FID mapping information for FID 1. In this case, no new mappings have been configured:

```
C3(su)->show spantree mstmap fid 1
```

```
FID:       SID:
1          0
```

set spantree mstmap

Use this command to map one or more filtering database IDs (FIDs) to a SID. Since VLANs are mapped to FIDs, this essentially maps one or more VLAN IDs to a Spanning Tree (SID).

Note: Since any MST maps that are associated with GVRP-generated VLANs will be removed from the configuration if GVRP communication is lost, it is recommended that you only create MST maps on statically-created VLANs.

Syntax

set spantree mstmap *fid* [**sid** *sid*]

Parameters

fid	Specifies one or more FIDs to assign to the MST. Valid values are **1** - **4093**, and must correspond to a VLAN ID created using the **set vlan** command.
sid *sid*	(Optional) Specifies a Multiple Spanning Tree ID. Valid values are **1** - **4094**, and must correspond to a SID created using the **set msti** command.

Defaults

If *sid* is not specified, FID(s) will be mapped to Spanning Tree 0.

Mode

Switch command, read-write.

Example

This example shows how to map FID 3 to SID 2:

```
C3(su)->set spantree mstmap 3 sid 2
```

clear spantree mstmap

Use this command to map a FID back to SID 0.

Syntax

clear spantree mstmap *fid*

Parameters

fid	Specifies one or more FIDs to reset to 0.

Defaults

If *fid* is not specified, all SID to FID mappings will be reset.

Mode

Switch command, read-write.

Example

This example shows how to map FID 2 back to SID 0:

```
C3(su)->clear spantree mstmap 2
```

show spantree vlanlist

Use this command to display the Spanning Tree ID(s) assigned to one or more VLANs.

Syntax

show spantree vlanlist [*vlan-list*]

Parameters

vlan-list	(Optional) Displays SIDs assigned to specific VLAN(s).

Defaults

If not specified, SID assignment will be displayed for all VLANs.

Mode

Switch command, read-only.

Example

This example shows how to display the SIDs mapped to VLAN 1. In this case, SIDs 2, 16 and 42 are mapped to VLAN 1. For this information to display, the SID instance must be created using the **set spantree msti** command as described in "set spantree msti" on page 9-12, and the FIDs must be mapped to SID 1 using the **set spantree mstmap** command as described in "set spantree mstmap" on page 9-14:

```
C3(su)->show spantree vlanlist 1
 The following SIDS are assigned to VLAN 1: 2 16 42
```

show spantree mstcfgid

Use this command to display the MST configuration identifier elements, including format selector, configuration name, revision level, and configuration digest.

Syntax

show spantree mstcfgid

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the MST configuration identifier elements. In this case, the default revision level of 0, and the default configuration name (a string representing the bridge MAC address) have not been changed. For information on using the **set spantree mstcfgid** command to change these settings, refer to "set spantree mstcfgid" on page 9-16:

```
C3(su)->show spantree mstcfgid
 MST Configuration Identifier:
  Format Selector: 0
  Configuration Name: 00:01:f4:89:51:94
  Revision Level: 0
  Configuration Digest: ac:36:17:7f:50:28:3c:d4:b8:38:21:d8:ab:26:de:62
```

set spantree mstcfgid

Use this command to set the MST configuration name and/or revision level.

Syntax

set spantree mstcfgid {**cfgname** *name* | **rev** *level*}

Parameters

cfgname *name*	Specifies an MST configuration name.
rev *level*	Specifies an MST revision level. Valid values are **0** - **65535**.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the MST configuration name to "mstconfig":

```
C3(su)->set spantree mstconfigid cfgname mstconfig
```

clear spantree mstcfgid

Use this command to reset the MST revision level to a default value of 0, and the configuration name to a default string representing the bridge MAC address.

Syntax

clear spantree mstcfgid

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the MST configuration identifier elements to default values:

```
C3(su)->clear spantree mstcfgid
```

set spantree priority

Use this command to set the device's Spanning Tree priority.

Syntax

set spantree priority *priority* [*sid*]

Parameters

priority	Specifies the priority of the bridge. Valid values are from **0** to **61440 (**in increments of 4096**)**, with 0 indicating highest priority and 61440 lowest priority.
sid	(Optional) Sets the priority on a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, priority will be set on Spanning Tree 0.

Mode

Switch command, read-write.

Usage

The device with the highest priority (lowest numerical value) becomes the Spanning Tree root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device. Depending on the bridge priority mode (set with the **set spantree bridgeprioritymode** command described in "set spantree bridgeprioritymode" on page 9-11, some priority values may be rounded up or down.

Example

This example shows how to set the bridge priority to 4096 on SID 1:

```
C3(su)->set spantree priority 4096 1
```

clear spantree priority

Use this command to reset the Spanning Tree priority to the default value of 32768.

Syntax

clear spantree priority [*sid*]

Parameters

sid	(Optional) Resets the priority on a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, priority will be reset on Spanning Tree 0.

Mode

Switch command, read-write.

Example

This example shows how to reset the bridge priority on SID 1:

```
C3(su)->clear spantree priority 1
```

set spantree hello

Use this command to set the device's Spanning Tree hello time, This is the time interval (in seconds) the device will transmit BPDUs indicating it is active.

Syntax

set spantree hello *interval*

Parameters

interval	Specifies the number of seconds the system waits before broadcasting a bridge hello message (a multicast message indicating that the system is active). Valid values are **1** - **10**.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to globally set the Spanning Tree hello time to 10 seconds:

```
C3(su)->set spantree hello 10
```

clear spantree hello

Use this command to reset the Spanning Tree hello time to the default value of 2 seconds.

Syntax

clear spantree hello

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to globally reset the Spanning Tree hello time:

```
C3(su)->clear spantree hello
```

set spantree maxage

Use this command to set the bridge maximum aging time.

Syntax

set spantree maxage *agingtime*

Parameters

agingtime	Specifies the maximum number of seconds that the system retains the information received from other bridges through STP. Valid values are **6** - **40**.

Defaults

None.

Mode

Switch command, read-write.

Usage

The bridge maximum aging time is the maximum time (in seconds) a device can wait without receiving a configuration message (bridge “hello”) before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information provided in the last configuration message becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

This example shows how to set the maximum aging time to 25 seconds:

```
C3(su)->set spantree maxage 25
```

clear spantree maxage

Use this command to reset the maximum aging time for a Spanning Tree to the default value of 20 seconds.

Syntax

clear spantree maxage

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to globally reset the maximum aging time:

```
C3(su)->clear spantree maxage
```

set spantree fwddelay

Use this command to set the Spanning Tree forward delay.

Syntax

set spantree fwddelay *delay*

Parameters

delay	Specifies the number of seconds for the bridge forward delay. Valid values are **4** - **30**.

Defaults

None.

Mode

Switch command, read-write.

Usage

The forward delay is the maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.

Example

This example shows how to globally set the bridge forward delay to 16 seconds:

```
C3(su)->set spantree fwddelay 16
```

clear spantree fwddelay

Use this command to reset the Spanning Tree forward delay to the default setting of 15 seconds.

Syntax

clear spantree fwddelay

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to globally reset the bridge forward delay:

```
C3(su)->clear spantree fwddelay
```

show spantree backuproot

Use this command to display the backup root status for an MST instance.

Syntax

show spantree backuproot [*sid*]

Parameters

sid	(Optional) Display backup root status for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If a SID is not specified, then status will be shown for Spanning Tree instance 0.

Mode

Switch command, read-only.

Example

This example shows how to display the status of the backup root function on SID 0:

```
C3(rw)->show spantree backuproot
Backup root is set to disable on sid 0
```

set spantree backuproot

Use this command to enable or disable the Spanning Tree backup root function on the switch.

Syntax

set spantree backuproot *sid* {disable | enable}

Parameters

sid	Specifies the Spanning Tree instance on which to enable or disable the backup root function.Valid values are **0** - **4094**.
disable | enable	Enables or disables the backup root function.

Defaults

None.

Mode

Switch command, read-write.

Usage

The Spanning Tree backup root function is disabled by default on the SecureStack C3. When this feature is enabled and the switch is directly connected to the root bridge, stale Spanning Tree information is prevented from circulating if the root bridge is lost. If the root bridge is lost, the backup root will dynamically lower its bridge priority so that it will be selected as the new root over the lost root bridge.

Example

This example shows how to enable the backup root function on SID 2:

```
C3(rw)->set spantree backuproot 2 enable
```

clear spantree backuproot

Use this command to reset the Spanning Tree backup root function to the default state of disabled.

Syntax

clear spantree backuproot *sid*

Parameters

sid	Specifies the Spanning Tree on which to clear the backup root function.Valid values are **0** - **4094**.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the backup root function to disabled on SID 2:

```
C3(rw)->clear spantree backuproot 2
```

show spantree tctrapsuppress

Use this command to display the status of topology change trap suppression on Rapid Spanning Tree edge ports.

Syntax

```
show spantree tctrapsuppress
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the status of topology change trap suppression:

```
C3(rw)->show spantree tctrapsuppress
Topology change Trap Suppression is set to enabled
```

set spantree tctrapsuppress

Use this command to disable or enable topology change trap suppression on Rapid Spanning Tree edge ports.

Syntax

```
set spantree tctrapsuppress {disable | enable}
```

Parameters

disable | **enable**	Disables or enables topology change trap suppression.

Defaults

None.

Mode

Switch command, read-write.

Usage

By default, RSTP non-edge (bridge) ports that transition to forwarding or blocking cause the switch to issue a topology change trap. When topology change trap suppression is enabled, which is the device default, edge ports (such as end station PCs) are prevented from sending topology change traps. This is because there is usually no need for network management to monitor edge port STP transition states, such as when PCs are powered on. When topology change trap suppression is disabled, all ports, including edge and bridge ports, will transmit topology change traps.

Example

This example shows how to allow Rapid Spanning Tree edge ports to transmit topology change traps:

```
C3(rw)->set spantree tctrapsuppress disable
```

clear spantree tctrapsuppress

Use this command to clear the status of topology change trap suppression on Rapid Spanning Tree edge ports to the default state of enabled (edge port topology changes do not generate traps).

Syntax

clear spantree tctrapsuppress

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear topology change trap suppression setting:

```
C3(rw)->clear spantree tctrapsuppress
```

set spantree protomigration

Use this command to reset the protocol state migration machine for one or more Spanning Tree ports. When operating in RSTP mode, this forces a port to transmit MSTP BPDUs.

Syntax

set spantree protomigration *<port-string>*

Parameters

port-string	Reset the protocol state migration machine for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the protocol state migration machine on port 20:

```
C3(su)->set spantree protomigration ge.1.20
```

show spantree spanguard

Use this command to display the status of the Spanning Tree SpanGuard function.

Syntax

```
show spantree spanguard
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the SpanGuard function status:

```
C3(su)->show spantree spanguard
Spanguard is disabled
```

set spantree spanguard

Use this command to enable or disable the Spanning Tree SpanGuard function.

Syntax

```
set spantree spanguard {enable | disable}
```

Parameters

enable | **disable**	Enables or disables the SpanGuard function.

Defaults

None.

Mode

Switch command, read-write.

Usage

SpanGuard is designed to disable, or lock out an "edge" port when an unexpected BPDU is received. The port can be configured to be re-enabled after a set time period, or only after manual intervention.

A port can be defined as an edge (user) port using the **set spantree adminedge** command, described in "set spantree adminedge" on page 9-40. A port designated as an edge port is expected to be connected to a workstation or other end-user type of device, and not to another switch in the network. When SpanGuard is enabled, if a non-loopback BPDU is received on an edge port, the Spanning Tree state of that port will be changed to "blocking" and will no longer forward traffic. The port will remain disabled until the amount of time defined by **set spantree spanguardtimeout** ("set spantree spanguardtimeout" on page 9-27) has passed since the last seen BPDU, the port is manually unlocked (**set** or **clear spantree spanguardlock**, "clear / set spantree spanguardlock" on page 9-29), the configuration of the port is changed so it is not longer an edge port, or the SpanGuard function is disabled.

SpanGuard is enabled and disabled only on a global basis (across the stack, if applicable). By default, SpanGuard is disabled and SpanGuard traps are enabled.

Example

This example shows how to enable the SpanGuard function:

```
C3(rw)->set spantree spanguard enable
```

clear spantree spanguard

Use this command to reset the status of the Spanning Tree SpanGuard function to disabled.

Syntax

```
clear spantree spanguard
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the status of the SpanGuard function to disabled:

```
C3(rw)->clear spantree spanguard
```

show spantree spanguardtimeout

Use this command to display the Spanning Tree SpanGuard timeout setting.

Syntax

show spantree spanguardtimeout

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the SpanGuard timeout setting:

```
C3(su)->show spantree spanguardtimeout
Spanguard timeout: 300
```

set spantree spanguardtimeout

Use this command to set the amount of time (in seconds) an edge port will remain locked by the SpanGuard function.

Syntax

set spantree spanguardtimeout *timeout*

Parameters

timeout	Specifies a timeout value in seconds. Valid values are **0** to **65535**. A value of 0 will keep the port locked until manually unlocked. The default value is 300 seconds.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the SpanGuard timeout to 600 seconds:

```
C3(su)->set spantree spanguardtimeout 600
```

clear spantree spanguardtimeout

Use this command to reset the Spanning Tree SpanGuard timeout to the default value of 300 seconds.

Syntax

```
clear spantree spanguardtimeout
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the SpanGuard timeout to 300 seconds:

```
C3(rw)->clear spantree spanguardtimeout
```

show spantree spanguardlock

Use this command to display the SpanGuard lock status of one or more ports.

Syntax

show spantree spanguardlock [*port-string*]

Parameters

port-string	(Optional) Specifies the port(s) for which to show SpanGuard lock status. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If no port string is specified, the SpanGuard lock status for all ports is displayed.

Mode

Switch command, read-only.

Example

This example shows how to display the SpanGuard lock status for ge.1.1:

```
C3(su)->show spantree spanguardlock ge.1.1
Port ge.1.1 is Unlocked
```

clear / set spantree spanguardlock

Use either of these commands to unlock one or more ports locked by the Spanning Tree SpanGuard function. When SpanGuard is enabled, it locks ports that receive BPDUs when those ports have been defined as edge (user) ports (as described in "set spantree adminedge" on page 9-40).

Syntax

```
clear spantree spanguardlock port-string
set spantree spanguardlock port-string
```

Parameters

port-string	Specifies port(s) to unlock. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to unlock port `ge.1.16`:

```
C3(rw)->clear spantree spanguardlock ge.1.16
```

show spantree spanguardtrapenable

Use this command to display the state of the Spanning Tree SpanGuard trap function.

Syntax

```
show spantree spanguardtrapenable
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the state of the SpanGuard trap function:

```
C3(ro)->show spantree spanguardtrapenable
Spanguard SNMP traps are enabled
```

set spantree spanguardtrapenable

Use this command to enable or disable the sending of an SNMP trap message when SpanGuard has locked a port.

Syntax

```
set spantree spanguardtrapenable {disable | enable}
```

Parameters

disable | **enable**	Disables or enables sending SpanGuard traps. By default, sending traps is enabled.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to disable the SpanGuard trap function:

```
C3(su)->set spantree spanguardtrapenable disable
```

clear spantree spanguardtrapenable

Use this command to reset the Spanning Tree SpanGuard trap function back to the default state of enabled.

Syntax

```
clear spantree spanguardtrapenable
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the SpanGuard trap function to enabled:

```
C3(rw)->clear spantree spanguardtrapenable
```

show spantree legacypathcost

Use this command to display the default Spanning Tree path cost setting.

Syntax

```
show spantree legacypathcost
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the default Spanning Tree path cost setting.

```
C3(su)->show spantree legacypathcost
Legacy Path Cost is disabled.
```

set spantree legacypathcost

Use this command to enable or disable legacy (802.1D) path cost values.

Syntax

```
set spantree legacypathcost {disable | enable}
```

Parameters

disable	Use 802.1t2001 values to calculate path cost.
enable	Use 802.1d1998 values to calculate path cost.

Defaults

None.

Mode

Switch command, read-write.

Usage

By default, legacy path cost is disabled. Enabling the device to calculate legacy path costs affects the range of valid values that can be entered in the **set spantree adminpathcost** command.

Example

This example shows how to set the default path cost values to 802.1D.

```
C3(rw)->set spantree legacypathcost enable
```

clear spantree legacypathcost

Use this command to set the Spanning Tree default value for legacy path cost to 802.1t values.

Syntax

clear spantree legacypathcost

Defaults

None.

Mode

Switch command, read-write.

Example

This example clears the legacy path cost to 802.1t values.

```
C3(rw)->clear spantree legacypathcost
```

show spantree autoedge

Use this command to display the status of automatic edge port detection.

Syntax

show spantree autoedge

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the status of the automatic edge port detection function:

```
C3(rw)->show spantree autoedge
  autoEdge is currently enabled.
```

set spantree autoedge

Use this command to enable or disable the automatic edge port detection function.

Syntax

set spantree autoedge {**disable** | **enable**}

Parameters

disable | **enable**	Disables or enables automatic edge port detection.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to disable automatic edge port detection:

```
C3(rw)->set spantree autoedge disable
```

clear spantree autoedge

Use this command to reset automatic edge port detection to the default state of enabled.

Syntax

```
clear spantree autoedge
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset automatic edge port detection to enabled:

```
C3(rw)->clear spantree autoedge
```

Configuring Spanning Tree Port Parameters

Purpose

To display and set Spanning Tree port parameters.

Commands

set spantree portadmin

Use this command to disable or enable the Spanning Tree algorithm on one or more ports.

Syntax

set spantree portadmin *port-string* **{disable | enable}**

Parameters

port-string	Specifies the port(s) for which to enable or disable Spanning Tree. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
disable | **enable**	Disables or enables Spanning Tree.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to disable Spanning Tree on ge.1.5:

```
C3(rw)->set spantree portadmin ge.1.5 disable
```

clear spantree portadmin

Use this command to reset the default Spanning Tree admin status to enable on one or more ports.

Syntax

clear spantree portadmin *port-string*

Parameters

port-string	Resets the default admin status on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the default Spanning Tree admin state to enable on ge.1.12:

```
C3(rw)->clear spantree portadmin ge.1.12
```

show spantree portadmin

Use this command to display the status of the Spanning Tree algorithm on one or more ports.

Syntax

show spantree portadmin [**port** *port-string]*

Parameters

port *port-string*	(Optional) Displays status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, status will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display port admin status for ge.1.1:

```
C3(ro)->show spantree portadmin port ge.1.1
Port ge.1.1 has portadmin set to enabled
```

show spantree portpri

Use this command to show the Spanning Tree priority for one or more ports. Port priority is a component of the port ID, which is one element used in determining Spanning Tree port roles.

Syntax

show spantree portpri [**port** *port-string*] [**sid** *sid*]

Parameters

port *port-string*	(Optional) Specifies the port(s) for which to display Spanning Tree priority. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
sid *sid*	(Optional) Displays port priority for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *port-string* is not specified, port priority will be displayed for all Spanning Tree ports.

If *sid* is not specified, port priority will be displayed for Spanning Tree 0.

Mode

Switch command, read-only.

Example

This example shows how to display the port priority for ge.2.7:

```
C3(su)->show spantree portpri port ge.2.7
Port ge.2.7 has a Port Priority of 128 on SID 0
```

set spantree portpri

Use this command to set a port's Spanning Tree priority.

Syntax

set spantree portpri *port-string priority* [**sid** *sid*]

Parameters

port-string	Specifies the port(s) for which to set Spanning Tree port priority. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
priority	Specifies a number that represents the priority of a link in a Spanning Tree bridge. Valid values are from **0** to **240 (in increments of 16)** with 0 indicating high priority.
sid *sid*	(Optional) Sets port priority for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, port priority will be set for Spanning Tree 0.

Mode

Switch command, read-write.

Example

This example shows how to set the priority of ge.1.3 to 240 on SID 1

```
C3(su)->set spantree portpri ge.1.3 240 sid 1
```

clear spantree portpri

Use this command to reset the bridge priority of a Spanning Tree port to a default value of 128.

Syntax

clear spantree portpri *port-string* [**sid** *sid*]

Parameters

port-string	Specifies the port(s) for which to set Spanning Tree port priority. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
sid *sid*	(Optional) Resets the port priority for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 will be assumed.

Defaults

If *sid* is not specified, port priority will be set for Spanning Tree 0.

Mode

Switch command, read-write.

Example

This example shows how to reset the priority of ge.1.3 to 128 on SID 1

```
C3(su)->clear spantree portpri ge.1.3 sid 1
```

show spantree adminpathcost

Use this command to display the admin path cost for a port on one or more Spanning Trees.

Syntax

show spantree adminpathcost [**port** *port-string*] [**sid** *sid*]

Parameters

port *port-string*	(Optional) Displays the admin path cost value for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
sid *sid*	(Optional) Displays the admin path cost for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 will be assumed.

Defaults

If *port-string* is not specified, admin path cost for all Spanning Tree ports will be displayed.

If *sid* is not specified, admin path cost for Spanning Tree 0 will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display the admin path cost for ge.3.4 on SID 1:

```
C3(su)->show spantree adminpathcost port ge.3.4 sid 1
Port ge.3.4 has a Port Admin Path Cost of 0 on SID 1
```

set spantree adminpathcost

Use this command to set the administrative path cost on a port and one or more Spanning Trees.

Syntax

set spantree adminpathcost *port-string cost* [**sid** *sid*]

Parameters

port-string	Specifies the port(s) on which to set an admin path cost. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
cost	Specifies the port path cost. Va1id values are **0** - **200000000**.
sid *sid*	(Optional) Sets the admin path cost for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 will be assumed.

Defaults

If *sid* is not specified, admin path cost will be set for Spanning Tree 0.

Mode

Switch command, read-write.

Example

This example shows how to set the admin path cost to 200 for ge.3.2 on SID 1:

```
C3(su)->set spantree adminpathcost ge.3.2 200 sid 1
```

clear spantree adminpathcost

Use this command to reset the Spanning Tree default value for port admin path cost to 0.

Syntax

clear spantree adminpathcost *port-string* [**sid** *sid*]

Parameters

port-string	Specifies the port(s) for which to reset admin path cost. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
sid *sid*	(Optional) Resets the admin path cost for specific Spanning Tree(s). Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, admin path cost will be reset for Spanning Tree 0.

Mode

Switch command, read-write.

Example

This example shows how to reset the admin path cost to 0 for ge.3.2 on SID 1:

```
C3(su)->clear spantree adminpathcost ge.3.2 sid 1
```

show spantree adminedge

Use this command to display the edge port administrative status for a port.

Syntax

show spantree adminedge [port *port-string*]

Parameters

port-string	(Optional) Displays edge port administrative status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified edge port administrative status will be displayed for all Spanning Tree ports.

Mode

Switch command, read-only.

Example

This example shows how to display the edge port status for ge.3.2:

```
C3(su)->show spantree adminedge port ge.3.2
Port ge.3.2 has a Port Admin Edge of Edge-Port
```

set spantree adminedge

Use this command to set the edge port administrative status on a Spanning Tree port.

Syntax

set spantree adminedge *port-string* **{true | false}**

Parameters

port-string	Specifies the edge port. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
true | **false**	Enables (**true**) or disables (**false**) the specified port as a Spanning Tree edge port.

Defaults

None.

Mode

Switch command, read-write.

Usage

The default behavior of the edge port administrative status begins with the value set to **false** initially after the device is powered up. If a Spanning Tree BDPU is not received on the port within a few seconds, the status setting changes to **true**.

Example

This example shows how to set ge.1.11 as an edge port:

```
C3(su)->set spantree adminedge ge.1.11 true
```

clear spantree adminedge

Use this command to reset a Spanning Tree port to non-edge status.

Syntax

clear spantree adminedge *port-string*

Parameters

port-string	Specifies port(s) on which to reset edge port status. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset ge.1.11 as a non-edge port:

```
C3(su)->clear spantree adminedge ge.1.11
```

show spantree operedge

Use this command to display the Spanning Tree edge port operating status for a port.

Syntax

show spantree operedge [**port** *port-string*]

Parameters

port *port-string*	Displays edge port operating status for specific port(s).

Defaults

If *port-string* is not specified, edge port operating status will be displayed for all Spanning Tree ports.

Mode

Switch command, read-only.

Example

This example shows how to display the edge port status for ge.2.7:

```
C3(rw)->show spantree operedge port ge.2.7
Port ge.2.7 has a Port Oper Edge of Edge-Port
```

Configuring Spanning Tree Loop Protect Parameters

Purpose

To display and set Spanning Tree Loop Protect parameters, including the global parameters of Loop Protect threshold, window, enabling traps, and disputed BPDU threshold, as well as per port and port/SID parameters. See "Loop Protect" on page 9-2 for more information about the Loop Protect feature.

Commands

For information about...	Refer to page...
set spantree lp	9-43
show spantree lp	9-43
clear spantree lp	9-44
show spantree lplock	9-44
clear spantree lplock	9-45
set spantree lpcapablepartner	9-46
show spantree lpcapablepartner	9-46
clear spantree lpcapablepartner	9-47
set spantree lpthreshold	9-47
show spantree lpthreshold	9-48
clear spantree lpthreshold	9-48
set spantree lpwindow	9-49
show spantree lpwindow	9-49
clear spantree lpwindow	9-50
set spantree lptrapenable	9-50
show spantree lptrapenable	9-51
clear spantree lptrapenable	9-51
set spantree disputedbpduthreshold	9-52
show spantree disputedbpduthreshold	9-53
clear spantree disputedbpduthreshold	9-53
show spantree nonforwardingreason	9-54

set spantree lp

Use this command to enable or disable the Loop Protect feature per port and optionally, per SID. The Loop Protect feature is disabled by default. See “Loop Protect” on page 2. for more information.

Syntax

set spantree lp *port-string* {**enable** | **disable**} [**sid** *sid*]

Parameters

port-string	Specifies port(s) on which to enable or disable the Loop Protect feature.
enable | **disable**	Enables or disables the feature on the specified port.
sid *sid*	(Optional) Enables or disables the feature for specific Spanning Tree(s). Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no SID is specified, SID 0 is assumed.

Mode

Switch command, read-write.

Usage

Loop Protect takes precedence over per port STP enable/disable (portAdmin). Normally portAdmin disabled would cause a port to go immediately to forwarding. If Loop Protect is enabled, that port should go to listening and remain there.

Note: The Loop Protect enable/disable settings for an MSTI port should match those for the CIST port.

Example

This example shows how to enable Loop Protect on ge.2.3:

```
C3(su)->set spantree lp ge.1.11 enable
```

show spantree lp

Use this command to display the Loop Protect status per port and/or per SID.

Syntax

show spantree lp [**port** *port-string*] [**sid** *sid*]

Parameters

port-string	(Optional) Specifies port(s) for which to display the Loop Protect feature status.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to display the Loop Protect feature status. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no *port-string* is specified, status is displayed for all ports.

If no SID is specified, SID 0 is assumed.

Mode

Switch command, read-only.

Example

This example shows how to display Loop Protect status on ge.2.3:

```
C3(su)->show spantree lp port ge.2.3
LoopProtect is disabled on port ge.2.3    , SI
```

clear spantree lp

Use this command to return the Loop Protect status per port and optionally, per SID, to its default state of disabled.

Syntax

clear spantree lp *port-string* [**sid** *sid*]

Parameters

port-string	Specifies port(s) for which to clear the Loop Protect feature status.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to clear the Loop Protect feature status. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no SID is specified, SID 0 is assumed.

Mode

Switch command, read-write.

Example

This example shows how to return the Loop Protect state on ge.2.3 to disabled:

```
C3(rw)->clear spantree lp port ge.2.3
```

show spantree lplock

Use this command to display the Loop Protect lock status per port and/or per SID. A port can become locked if a configured number of Loop Protect events occur during the configured window of time. See the set spantree lpthreshold and set spantree lpwindow commands. Once a port is forced into blocking (locked), it remains locked until manually unlocked with the clear spantree lplock command.

Syntax

show spantree lplock [**port** *port-string*] [**sid** *sid*]

Parameters

port-string	(Optional) Specifies port(s) for which to display the Loop Protect lock status.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to display the Loop Protect lock status. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no *port-string* is specified, status is displayed for all ports.

If no SID is specified, SID 0 is assumed.

Mode

Switch command, read-only.

Example

This example shows how to display Loop Protect lock status on ge.1.1:

```
C3(rw)->show spantree lplock port ge.1.1
The LoopProtect lock status for port ge.1.1     , SID 0 is UNLOCKED
```

clear spantree lplock

Use this command to manually unlock a blocked port and optionally, per SID. The default state is unlocked.

Syntax

clear spantree lplock *port-string* [**sid** *sid*]

Parameters

port-string	Specifies port(s) for which to clear the Loop Protect lock.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to clear the Loop Protect lock. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no SID is specified, SID 0 is assumed.

Mode

Switch command, read-only.

Example

This example shows how to clear Loop Protect lock from ge.1.1:

```
C3(rw)->show spantree lplock port ge.1.1
The LoopProtect lock status for port ge.1.1     , SID 0 is LOCKED
C3(rw)->clear spantree lplock ge.1.1
C3(rw)->show spantree lplock port ge.1.1
The LoopProtect lock status for port ge.1.1     , SID 0 is UNLOCKED
```

set spantree lpcapablepartner

Use this command to specify per port whether the link partner is Loop Protect capable. See “Loop Protect” on page 2. for more information.

Syntax

set spantree lpcapablepartner *port-string* {**true** | **false**}

Parameters

port-string	Specifies port(s) for which to configure a Loop Protect capable link partner.
true | **false**	Specifies whether the link partner is capable (true) or not (false).

Defaults

None.

Mode

Switch command, read-write.

Usage

The default value for Loop Protect capable partner is false. If the port is configured with a Loop Protect capable partner (true), then the full functionality of the Loop Protect feature is used. If the value is false, then there is some ambiguity as to whether an Active Partner timeout is due to a loop protection event or is a normal situation due to the fact that the partner port does not transmit Alternate Agreement BPDUs. Therefore, a conservative approach is taken in that designated ports will not be allowed to forward unless receiving agreements from a port with root role.

This type of timeout will not be considered a loop protection event. Loop protection is maintained by keeping the port from forwarding but since this is not considered a loop event it will not be factored into locking the port.

Example

This example shows how to set the Loop Protect capable partner to true for ge.1.1:

```
C3(rw)->set spantree lpcapablepartner ge.1.1 true
```

show spantree lpcapablepartner

Use this command to the Loop Protect capability of a link partner for one or more ports.

Syntax

show spantree lpcapablepartner [**port** *port-string*]

Parameters

port-string	(Optional) Specifies port(s) for which to display Loop Protect capability for its link partner.

Defaults

If no *port-string* is specified, Loop Protect capability for link partners is displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display the Loop Protect partner capability for ge.1.1:

```
C3(rw)->show spantree lpcapablepartner port ge.1.1
Link partner of port ge.1.1 is not LoopProtect-capable
```

clear spantree lpcapablepartner

Use this command to reset the Loop Protect capability of port link partners to the default state of false.

Syntax

clear spantree lpcapablepartner *port-string*

Parameters

port-string	Specifies port(s) for which to clear their link partners' Loop Protect capability (reset to false).

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the Loop Protect partner capability for ge.1.1:

```
C3(rw)->clear spantree lpcapablepartner ge.1.1
```

set spantree lpthreshold

Use this command to set the Loop Protect event threshold.

Syntax

set spantree lpthreshold *value*

Parameters

value	Specifies the number of events that must occur during the event window in order to lock a port/SID. The default value is 3 events. A threshold of 0 specifies that ports will never be locked.

Defaults

None. The default event threshold is 3.

Mode

Switch command, read-write.

Usage

The LoopProtect event threshold is a global integer variable that provides protection in the case of intermittent failures. The default value is 3. If the event counter reaches the threshold within a given period (the event window), then the port, for the given SID, becomes locked (that is, held indefinitely in the blocking state). If the threshold is 0, the ports are never locked.

Example

This example shows how to set the Loop Protect threshold value to 4:

```
C3(rw)->set spantree lpthreshold 4
```

show spantree lpthreshold

Use this command to display the current value of the Loop Protect event threshold.

Syntax

`show spantree lpthreshold`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the current Loop Protect threshold value:

```
C3(rw)->show spantree lpthreshold
The Loop Protect event threshold value is 4
```

clear spantree lpthreshold

Use this command to return the Loop Protect event threshold to its default value of 3.

Syntax

`clear spantree lpthreshold`

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the Loop Protect event threshold to the default of 3:

```
C3(rw)->clear spantree lpthreshold
```

set spantree lpwindow

Use this command to set the Loop Protect event window value in seconds.

Syntax

`set spantree lpwindow` *`value`*

Parameters

value	Specifies the number of seconds that comprise the period during which Loop Protect events are counted. The default event window is 180 seconds.

Defaults

None.

Mode

Switch command, read-write.

Usage

The Loop Protect Window is a timer value, in seconds, that defines a period during which Loop Protect events are counted. The default value is 180 seconds. If the timer is set to 0, the event counter is not reset until the Loop Protect event threshold is reached. If the threshold is reached, that constitutes a loop protection event.

Example

This example shows how to set the Loop Protect event window to 120 seconds:

```
C3(rw)->set spantree lpwindow 120
```

show spantree lpwindow

Use this command to display the current Loop Protect event window value.

Syntax

`show spantree lpwindow`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the current Loop Protect window value:

```
C3(rw)->show spantree lpwindow
The Loop Protect event window is set to 120 seconds
```

clear spantree lpwindow

Use this command to reset the Loop Protect event window to the default value of 180 seconds.

Syntax

clear spantree lpwindow

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the Loop Protect event window to the default of 180 seconds:

```
C3(rw)->clear spantree lpwindow
```

set spantree lptrapenable

Use this command to enable or disable Loop Protect event notification.

Syntax

set spantree lptrapenable {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the sending of Loop Protect traps. Default is disabled.

Defaults

None.

Mode

Switch command, read-write.

Usage

Loop Protect traps are sent when a Loop Protect event occurs, that is, when a port goes to listening due to not receiving BPDUs. The trap indicates port, SID and loop protection status.

Example

This example shows how to enable sending of Loop Protect traps:

```
C3(rw)->set spantree lptrapenable enable
```

show spantree lptrapenable

Use this command to display the current status of Loop Protect event notification.

Syntax

`show spantree lptrapenable`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the current Loop Protect event notification status:

```
C3(rw)->show spantree lptrapenable
The Loop Protect event notification status is enable
```

clear spantree lptrapenable

Use this command to return the Loop Protect event notification state to its default state of disabled.

Syntax

`clear spantree lptrapenable`

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the Loop Protect event notification state to the default of disabled.

```
C3(rw)->clear spantree lptrapenable
```

set spantree disputedbpduthreshold

Use this command to set the disputed BPDU threshold, which is the number of disputed BPDUs that must be received on a given port/SID until a disputed BPDU trap is sent.

Syntax

`set spantree disputedbpduthreshold` *`value`*

Parameters

value	Specifies the number of disputed BPDUs that must be received on a given port/SID to cause a disputed BPDU trap to be sent. A threshold of 0 indicates that traps should not be sent. The default value is 0.

Defaults

None.

Mode

Switch command, read-write.

Usage

A disputed BPDU is one in which the flags field indicates a designated role and learning, and the priority vector is worse than that already held by the port. If a disputed BPDU is received the port is forced to the listening state. Refer to the 802.1Q-2005 standard, *IEEE Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks,* for a full description of the dispute mechanism, which prevents looping in cases of one-way communication.

The disputed BPDU threshold is an integer variable that represents the number of disputed BPDUs that must be received on a given port/SID until a disputed BPDU trap is sent and a syslog message is issued. For example, if the threshold is 10, then a trap is issued when 10, 20, 30, and so on, disputed BPDUs have been received.

If the value is 0, traps are not sent. The trap indicates port, SID and total Disputed BPDU count. The default is 0.

Example

This example shows how to set the disputed BPDU threshold value to 5:

```
C3(rw)->set spantree disputedbpduthreshold 5
```

show spantree disputedbpduthreshold

Use this command to display the current value of the disputed BPDU threshold.

Syntax

show spantree disputedbpduthreshold

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the current disputed BPDU threshold:

```
C3(rw)->show spantree disputedbpduthreshold
The disputed BPDU threshold value is 0
```

clear spantree disputedbpduthreshold

Use this command to return the disputed BPDU threshold to its default value of 0, meaning that disputed BPDU traps should not be sent.

Syntax

clear spantree disputedbpduthreshold

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the disputed BPDU threshold to the default of 0:

```
C3(rw)->clear spantree disputedbpduthreshold
```

show spantree nonforwardingreason

Use this command to display the reason for placing a port in a non-forwarding state due to an exceptional condition.

Syntax

show spantree nonforwardingreason *port-string* [**sid** *sid*]

Parameters

port-string	Specifies port(s) for which to display the non-forwarding reason.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to display the non-forwarding reason. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no *port-string* is specified, non-forwarding reason is displayed for all ports.

If no SID is specified, SID 0 is assumed.

Mode

Switch command, read-only.

Usage

Exceptional conditions causing a port to be placed in listening or blocking state include a Loop Protect event, receipt of disputed BPDUs, and loopback detection.

Example

This example shows how to display the non-forwarding reason on ge.1.1:

```
C3(rw)->show spantree nonforwardingreason port ge.1.1
The non-forwarding reason for port ge.1.1     on SID 0 is None
```

10

802.1Q VLAN Configuration

This chapter describes the SecureStack C3 system's capabilities to implement 802.1Q virtual LANs (VLANs).

Note: An Enterasys Networks Feature Guide document containing an in-depth discussion of VLAN configuration is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

VLAN Configuration Summary

Virtual LANs allow the network administrator to partition network traffic into logical groups and control the flow of that traffic through the network. Once the traffic and, in effect, the users creating the traffic, are assigned to a VLAN, then broadcast and multicast traffic is contained within the VLAN and users can be allowed or denied access to any of the network's resources. Also, some or all of the ports on the device can be configured as GVRP ports, which enable frames received with a particular VLAN ID and protocol to be transmitted on a limited number of ports. This keeps the traffic associated with a particular VLAN and protocol isolated from the other parts of the network.

Note: The device can support up to 1024 802.1Q VLANs. The allowable range for VLAN IDs is 1 to 4093. As a default, all ports on the device are assigned to VLAN ID 1, untagged.

Port String Syntax Used in the CLI

For information on how to designate VLANs and port numbers in the CLI syntax, refer to "Port String Syntax Used in the CLI" on page 7-1.

Creating a Secure Management VLAN

By default at startup, there is one VLAN configured on the SecureStack C3 device. It is VLAN ID 1, the DEFAULT VLAN. The default community name, which determines remote access for SNMP management, is set to "public" with read-write access.

If the SecureStack C3 device is to be configured for multiple VLANs, it may be desirable to configure a management-only VLAN. This allows a station connected to the management VLAN to manage the device. It also makes management secure by preventing configuration via ports assigned to other VLANs.

To create a secure management VLAN, you must:

Step	Task	Refer to page...
1.	Create a new VLAN.	10-5
2.	Set the PVID for the desired switch port to the VLAN created in Step 1.	10-9
3.	Add the desired switch port to the egress list for the VLAN created in Step 1.	10-15
4.	Assign host status to the VLAN.	10-18
5.	Set a private community name and access policy.	8-14

The commands used to create a secure management VLAN are listed in Table 10-1. This example assumes the management station is attached to ge.1.1 and wants untagged frames.

The process described here would be repeated on every device that is connected in the network to ensure that each device has a secure management VLAN.

Table 10-1 Command Set for Creating a Secure Management VLAN

To do this...	Use these commands...
Create a new VLAN and confirm settings.	**set vlan create 2** ("set vlan" on page 10-5)
	(Optional) **show vlan 2** ("show vlan" on page 10-3)
Set the PVID to the new VLAN.	**set port vlan ge.1.1 2** ("set port vlan" on page 10-9)
Add the port to the new VLAN's egress list.	**set vlan egress 2 ge.1.1 untagged** ("set vlan egress" on page 10-15)
Remove the port from the default VLAN's egress list.	**clear vlan egress 1 ge.1.1** ("clear vlan egress" on page 10-15)
Assign host status to the VLAN.	**set host vlan 2** ("set host vlan" on page 10-18)
Set a private community name and access policy and confirm settings.	**set snmp community private** ("set snmp community" on page 8-14)
	(Optional) **show snmp community** ("show snmp community" on page 8-13)

Viewing VLANs

Purpose

To display a list of VLANs currently configured on the device, to determine how one or more VLANs were created, the ports allowed and disallowed to transmit traffic belonging to VLAN(s), and if those ports will transmit the traffic with a VLAN tag included.

Command

For information about...	Refer to page...
show vlan	10-3

show vlan

Use this command to display all information related to one or more VLANs.

Syntax

show vlan [**static**] [*vlan-list*] [**portinfo** [**vlan** *vlan-list* | *vlan-name*] [**port** *port-string*]]

Parameters

static	(Optional) Displays information related to static VLANs. Static VLANs are manually created using the **set vlan** command ("set vlan" on page 10-5), SNMP MIBs, or the WebView management application. The default VLAN, VLAN 1, is always statically configured and can't be deleted. Only ports that use a specified VLAN as their default VLAN (PVID) will be displayed.
vlan-list	(Optional) Displays information for a specific VLAN or range of VLANs.
portinfo	(Optional) Displays VLAN attributes related to one or more ports.
vlan *vlan-list* | *vlan-name*	(Optional) Displays port information for one or more VLANs.
port *port-string*	(Optional) Displays port information for one or more ports.

Defaults

If no options are specified, all information related to static and dynamic VLANs will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display information for VLAN 1. In this case, VLAN 1 is named "DEFAULT VLAN". Ports allowed to transmit frames belonging to VLAN 1 are listed as egress ports. Ports that won't include a VLAN tag in their transmitted frames are listed as untagged ports. There are no forbidden ports (prevented from transmitted frames) on VLAN 1:

```
C3(su)->show vlan 1
 VLAN: 1         NAME: DEFAULT VLAN
```

```
 VLAN Type: Default
Egress Ports
ge.1.1-10, ge.2.1-4, ge.3.1-7,
 Forbidden Egress Ports
None.
 Untagged Ports
ge.1.1-10, ge.2.1-4, ge.3.1-7,
```

Table 10-2 provides an explanation of the command output.

Table 10-2 show vlan Output Details

Output Field	What It Displays...
VLAN	VLAN ID.
NAME	Name assigned to the VLAN.
Status	Whether it is **enabled** or **disabled**.
VLAN Type	Whether it is **permanent** (static) or **dynamic**.
Egress Ports	Ports configured to transmit frames for this VLAN.
Forbidden Egress Ports	Ports prevented from transmitting frames for this VLAN.
Untagged Ports	Ports configured to transmit untagged frames for this VLAN.

Creating and Naming Static VLANs

Purpose

To create a new static VLAN, or to enable or disable existing VLAN(s).

Commands

set vlan

Use this command to create a new static IEEE 802.1Q VLAN, or to enable or disable an existing VLAN.

Syntax

`set vlan {create | enable | disable}` *`vlan-list`*

Parameters

create | **enable** | **disable**	Creates, enables or disables VLAN(s).
vlan-list	Specifies one or more VLAN IDs to be created, enabled or disabled.

Defaults

None.

Mode

Switch command, read-write.

Usage

Once a VLAN is created, you can assign it a name using the **set vlan name** command described in "set vlan name" on page 10-6.

Each VLAN ID must be unique. If a duplicate VLAN ID is entered, the device assumes that the Administrator intends to modify the existing VLAN.

Enter the VLAN ID using a unique number between 1 and 4093. The VLAN IDs of 0 and 4094 and higher may not be used for user-defined VLANs.

Examples

This example shows how to create VLAN 3:

```
C3(su)->set vlan create 3
```

set vlan name

Use this command to set or change the ASCII name for a new or existing VLAN.

Syntax

set vlan name *vlan-list vlan-name*

Parameters

vlan-list	Specifies the VLAN ID of the VLAN(s) to be named.
vlan-name	Specifies the string used as the name of the VLAN (1 to 32 characters).

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the name for VLAN 7 to green:

```
C3(su)->set vlan name 7 green
```

clear vlan

Use this command to remove a static VLAN from the list of VLANs recognized by the device.

Syntax

clear vlan *vlan-list*

Parameters

vlan-list	Specifies the VLAN ID of the VLAN(s) to be removed.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to remove a static VLAN 9 from the device's VLAN list:

```
C3(su)->clear vlan 9
```

clear vlan name

Use this command to remove the name of a VLAN from the VLAN list.

Syntax

clear vlan name *vlan-list*

Parameters

vlan-list	Specifies the VLAN ID of the VLAN(s) for which the name will be cleared.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the name for VLAN 9:

```
C3(su)->clear vlan name 9
```

Assigning Port VLAN IDs (PVIDs) and Ingress Filtering

Purpose

To assign default VLAN IDs to untagged frames on one or more ports, to configure VLAN ingress filtering and constraints, and to set the frame discard mode.

Commands

show port vlan

Use this command to display port VLAN identifier (PVID) information. PVID determines the VLAN to which all untagged frames received on one or more ports will be classified.

Syntax

show port vlan [*port-string*]

Parameters

port-string	(Optional) Displays PVID information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port -string* is not specified, port VLAN information for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display PVIDs assigned to ge.2.1 through 6. In this case, untagged frames received on these ports will be classified to VLAN 1:

```
C3(su)->show port vlan ge.2.1-6
ge.2.1 is set to 1
ge.2.2 is set to 1
ge.2.3 is set to 1
ge.2.4 is set to 1
```

```
ge.2.5 is set to 1
ge.2.6 is set to 1
```

set port vlan

Use this command to configure the PVID (port VLAN identifier) for one or more ports.

Syntax

`set port vlan` *`port-string pvid`* **`[modify-egress | no-modify-egress]`**

Parameters

port-string	Specifies the port(s) for which to configure a VLAN identifier. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
pvid	Specifies the VLAN ID of the VLAN to which port(s) will be added.
modify-egress	(Optional) Adds port(s) to VLAN's untagged egress list and removes them from other untagged egress lists.
no-modify-egress	(Optional) Does not prompt for or make egress list changes.

Defaults

None.

Mode

Switch command, read-write.

Usage

The PVID is used to classify untagged frames as they ingress into a given port.

Example

This example shows how to add `ge.1.10` to the port VLAN list of VLAN 4 (PVID 4).

```
C3(su)->set vlan create 4
C3(su)->set port vlan ge.1.10 4 modify-egress
```

clear port vlan

Use this command to reset a port's 802.1Q port VLAN ID (PVID) to the host VLAN ID 1.

Note: The following command will reset the specified port's egress status to tagged. To set the specified ports back to the default egress status of untagged, you must issue the **set port vlan** command as described on page 10-9.

Syntax

`clear port vlan` *`port-string`*

Parameters

port-string	Specifies the port(s) to be reset to the host VLAN ID 1. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset ports `ge.1.3` through 11 to a VLAN ID of 1 (Host VLAN):

```
C3(su)->clear port vlan ge.1.3-11
```

show port ingress filter

Use this command to show all ports that are enabled for port ingress filtering, which limits incoming VLAN ID frames according to a port VLAN egress list. If the VLAN ID specified in the received frame is not on the port's VLAN egress list, then that frame is dropped and not forwarded.

Syntax

`show port ingress-filter` [*`port-string`*]

Parameters

port-string	(Optional) Specifies the port(s) for which to display ingress filtering status. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, ingress filtering status for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display the port ingress filter status for ports 10 through 15 in slot 1. In this case, the ports are disabled for ingress filtering:

```
C3(su)->show port ingress-filter ge.1.10-15
   Port      State
 --------  ---------
  ge.1.10  disabled
  ge.1.11  disabled
  ge.1.12  disabled
  ge.1.13  disabled
  ge.1.14  disabled
  ge.1.15  disabled
```

set port ingress filter

Use this command to discard all frames received with a VLAN ID that don't match the port's VLAN egress list.

Syntax

set port ingress-filter *port-string* {disable | enable}

Parameters

port-string	Specifies the port(s) on which to enable of disable ingress filtering. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
disable | **enable**	Disables or enables ingress filtering.

Defaults

None.

Mode

Switch command, read-write.

Usage

When ingress filtering is enabled on a port, the VLAN IDs of incoming frames are compared to the port's egress list. If the received VLAN ID does not match a VLAN ID on the port's egress list, then the frame is dropped.

Ingress filtering is implemented according to the IEEE 802.1Q standard.

Example

This example shows how to enable port ingress filtering on ge.1.3:

```
C3(su)->set port ingress-filter ge.1.3 enable
```

show port discard

Use this command to display the frame discard mode for one or more ports. Ports can be set to discard frames based on whether or not the frame contains a VLAN tag. They can also be set to discard both tagged and untagged frames, or neither.

Syntax

show port discard [*port-string*]

Parameters

port-string	(Optional) Displays the frame discard mode for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, frame discard mode will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display the frame discard mode for ge.2.7. In this case, the port has been set to discard all tagged frames:

```
C3(su)->show port discard ge.2.7
 Port         Discard Mode
------------  -------------
 ge.2.7         tagged
```

set port discard

Use this command to set the frame discard mode on one or more ports.

Syntax

set port discard *port-string* {**tagged** | **untagged** | **both** | **none**}

Parameters

port-string	Specifies the port(s) for which to set frame discard mode. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
tagged | **untagged** | **both** | **none**	• Tagged - Discard all incoming (received) tagged packets on the defined port(s). • Untagged - Discard all incoming untagged packets. • Both - All traffic will be discarded (tagged and untagged). • None - No packets will be discarded.

Defaults

None.

Mode

Switch command, read-write.

Usage

The options are to discard all incoming tagged frames, all incoming untagged frames, neither (essentially allow all traffic), or both (essentially discarding all traffic).

A common practice is to discard all tagged packet on user ports. Typically an Administrator does not want the end users defining what VLAN they use for communication.

Example

This example shows how to discard all tagged frames received on port ge.3.3:

```
C3(su)->set port discard ge.3.3 tagged
```

Configuring the VLAN Egress List

Purpose

To assign or remove ports on the egress list of a particular VLAN. This determines which ports on the switch will be eligible to transmit frames for a particular VLAN. For example, ports 1, 5, 7, 8 could be allowed to transmit frames belonging to VLAN 20 and ports 7,8, 9, 10 could be allowed to transmit frames tagged with VLAN 30 (a port can belong to multiple VLAN Egress lists). Note that the Port Egress list for ports 7 and 8 would contain both VLAN 20 and 30.

The port egress type for all ports can be set to tagged, forbidden, or untagged. In general, VLANs have no egress (except for VLAN 1) until they are configured by static administration, or through dynamic mechanisms such as GVRP.

Setting a port to forbidden prevents it from participating in the specified VLAN and ensures that any dynamic requests (either through GVRP or dynamic egress) for the port to join the VLAN will be ignored. Setting a port to untagged allows it to transmit frames without a tag header. This setting is usually used to configure a port connected to an end user device. Frames sent between VLAN aware switches are typically tagged.

The default VLAN defaults its egress to untagged for all ports.

Commands

show port egress

Use this command to display the VLAN membership for one or more ports.

Syntax

show port egress [*port-string*]

Parameters

port-string	(Optional) Displays VLAN membership for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, VLAN membership will be displayed for all ports.

Mode

Switch command, read-write.

Example

This example shows you how to show VLAN egress information for `ge.1.1` through 3. In this case, all three ports are allowed to transmit VLAN 1 frames as tagged and VLAN 10 frames as untagged. Both are static VLANs:

```
C3(su)->show port egress ge.1.1-3
 Port      Vlan          Egress     Registration
Number      Id           Status       Status
-------------------------------------------------------
ge.1.1       1           tagged       static
ge.1.1      10          untagged      static
ge.1.2       1           tagged       static
ge.1.2      10          untagged      static
ge.1.3       1           tagged       static
ge.1.3      10          untagged      static
```

set vlan forbidden

Use this command to prevent one or more ports from participating in a VLAN. This setting instructs the device to ignore dynamic requests (either through GVRP or dynamic egress) for the port to join the VLAN.

Syntax

`set vlan forbidden` *`vlan-id port-string`*

Parameters

vlan-id	Specifies the VLAN for which to set forbidden port(s).
port-string	Specifies the port(s) to set as forbidden for the specified *vlan-id*.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows you how to set `ge.1.3` to forbidden for VLAN 6:

```
C3(su)->set vlan forbidden 6 ge.1.3
```

set vlan egress

Use this command to add ports to the VLAN egress list for the device, or to prevent one or more ports from participating in a VLAN. This determines which ports will transmit frames for a particular VLAN.

Syntax

`set vlan egress` *`vlan-list port-string`* [**`untagged | forbidden | tagged`**]

Parameters

vlan-list	Specifies the VLAN where a port(s) will be added to the egress list.
port-string	Specifies one or more ports to add to the VLAN egress list of the specified *vlan-list*. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
untagged | **forbidden** | **tagged**	(Optional) Adds the specified ports as: • **untagged** — Causes the port(s) to transmit frames without an IEEE 802.1Q header tag. • **forbidden** — Instructs the device to ignore dynamic requests (either through GVRP or dynamic egress) from the port(s) to join the VLAN and disallows egress on that port. • **tagged** — Causes the port(s) to transmit 802.1Q tagged frames.

Defaults

If **untagged, forbidden** or **tagged** is not specified, the port will be added to the VLAN egress list as tagged.

Mode

Switch command, read-write.

Examples

This example shows how to add `ge.1.5` through 10 to the egress list of VLAN 7. This means that these ports will transmit VLAN 7 frames as tagged:

```
C3(su)->set vlan egress 7 ge.1.5-10 untagged
```

This example shows how to forbid ports 13 through 15 in slot 1 from joining VLAN 7 and disallow egress on those ports:

```
C3(su)->set vlan egress 7 ge.1.13-15 forbidden
```

This example shows how to allow port 2 in slot 1 to transmit VLAN 7 frames as untagged:

```
C3(su)->set vlan egress 7 ge.1.2 untagged
```

clear vlan egress

Use this command to remove ports from a VLAN's egress list.

Note: The following command will reset the specified port's egress status to tagged. To set the specified ports back to the default egress status of untagged, you must issue the **set vlan egress** command as described on page 10-15.

Syntax

clear vlan egress *vlan-list port-string* [**forbidden**]

Parameters

vlan-list	Specifies the number of the VLAN from which a port(s) will be removed from the egress list.
port-string	Specifies one or more ports to be removed from the VLAN egress list of the specified *vlan-list*. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
forbidden	(Optional) Clears the forbidden setting from the specified port(s) and resets the port(s) as able to egress frames if so configured by either static or dynamic means.

Defaults

If **forbidden** is not specified, tagged and untagged settings will be cleared.

Mode

Switch command, read-write.

Examples

This example shows how to remove ge.3.14 from the egress list of VLAN 9:

```
C3(su)->clear vlan egress 9 ge.3.14
```

This example shows how to remove all Ethernet ports in slot 2 from the egress list of VLAN 4:

```
C3(su)->clear vlan egress 4 ge.2.*
```

show vlan dynamicegress

Use this command to display the status of dynamic egress (enabled or disabled) for one or more VLANs.

Syntax

show vlan dynamicegress [*vlan-list*]

Parameters

vlan-list	(Optional) Displays dynamic egress status for specific VLAN(s).

Defaults

If *vlan-list* is not specified, the dynamic egress status for all VLANs will be displayed.

Mode

Switch command, read-write.

Example

This example shows how to display the dynamic egress status for VLANs 50-55:

```
C3(rw)->show vlan dynamicegress 50-55
VLAN 50 is disabled
VLAN 51 is disabled
VLAN 52 is disabled
VLAN 53 is enabled
VLAN 54 is enabled
VLAN 55 is enabled
```

set vlan dynamicegress

Use this command to administratively set the dynamic egress status for one or more VLANs.

Syntax

set vlan dynamicegress *vlan-list* **{enable | disable}**

Parameters

vlan-list	Specifies the VLANs by ID to enable or disable dynamic egress.
enable | **disable**	Enables or disables dynamic egress.

Defaults

None.

Mode

Switch command, read-write.

Usage

If dynamic egress is enabled for a particular VLAN, when a port receives a frame tagged with that VLAN's ID, the switch will add the receiving port to that VLAN's egress list. Dynamic egress is disabled on the SecureStack C3 by default.

For example, assume you have 20 AppleTalk users on your network who are mobile users (that is, use different ports every day), but you want to keep the AppleTalk traffic isolated in its own VLAN. You can create an AppleTalk VLAN with a VLAN ID of 55 with a classification rule that all AppleTalk traffic gets tagged with VLAN ID 55. Then, you enable dynamic egress for VLAN 55. Now, when an AppleTalk user plugs into port ge.3.5 and sends an AppleTalk packet, the switch will tag the packet to VLAN 55 and also add port ge.3.5 to VLAN 55's egress list, which allows the AppleTalk user to receive AppleTalk traffic.

Example

This example shows how to enable dynamic egress on VLAN 55:

```
C3(rw)->set vlan dynamicegress 55 enable
```

Setting the Host VLAN

Purpose

To configure a host VLAN that only select devices are allowed to access. This secures the host port for management-only tasks.

Note: The host port is the management entity of the device. Refer to “Creating a Secure Management VLAN” on page 10-2 for more information.

Commands

For information about...	Refer to page...
show host vlan	10-18
set host vlan	10-18
clear host vlan	10-19

show host vlan

Use this command to display the current host VLAN.

Syntax

show host vlan

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the host VLAN:

```
C3(su)->show host vlan
  Host vlan is 7.
```

set host vlan

Use this command to assign host status to a VLAN.

Syntax

set host vlan *vlan-id*

Parameters

vlan-id	Specifies the number of the VLAN to set as the host VLAN.

Defaults

None.

Mode

Switch command, read-write.

Usage

The host VLAN should be a secure VLAN where only designated users are allowed access. For example, a host VLAN could be specifically created for device management. This would allow a management station connected to the management VLAN to manage all ports on the device and make management secure by preventing management via ports assigned to other VLANs.

Note: Before you can designate a VLAN as the host VLAN, you must create a VLAN using the set of commands described in "Creating and Naming Static VLANs" on page 10-5.

Example

This example shows how to set VLAN 7 as the host VLAN:

```
C3(su)->set host vlan 7
```

clear host vlan

Use this command to reset the host VLAN to the default setting of 1.

Syntax

```
clear host vlan
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the host VLAN to the default setting:

```
C3(su)->clear host vlan
```

Enabling/Disabling GVRP (GARP VLAN Registration Protocol)

About GARP VLAN Registration Protocol (GVRP)

The following sections describe the device operation when its ports are operating under the Generic Attribute Registration Protocol (GARP) application – GARP VLAN Registration Protocol (GVRP).

Overview

The purpose of GVRP is to dynamically create VLANs across a switched network. When a VLAN is declared, the information is transmitted out GVRP configured ports on the device in a GARP formatted frame using the GVRP multicast MAC address. A switch that receives this frame, examines the frame, and extracts the VLAN IDs. GVRP then creates the VLANs and adds the receiving port to its tagged member list for the extracted VLAN ID (s). The information is then transmitted out the other GVRP configured ports of the device. Figure 10-1 shows an example of how VLAN blue from end station A would be propagated across a switch network.

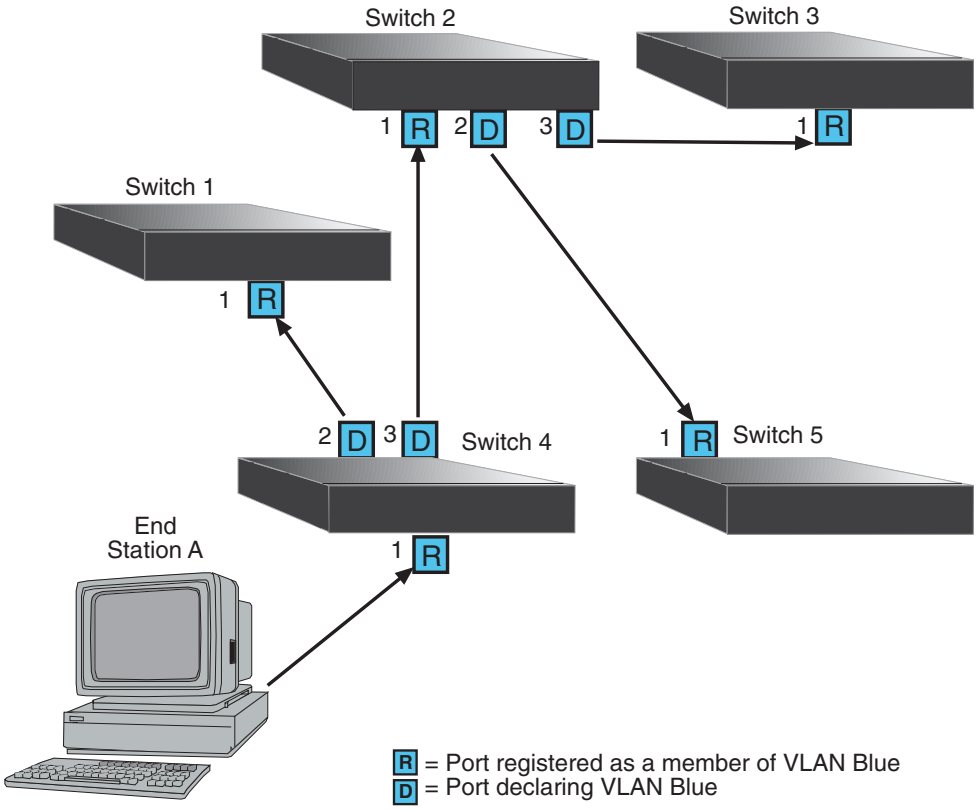
How It Works

In Figure 10-1 on page 10-21, Switch 4, port 1 is registered as being a member of VLAN Blue and then declares this fact out all its ports (2 and 3) to Switch 1 and Switch 2. These two devices register this in the port egress lists of the ports (Switch 1, port 1 and Switch 2, port 1) that received the frames with the information. Switch 2, which is connected to Switch 3 and Switch 5 declares the same information to those two devices and the port egress list of each port is updated with the new information, accordingly.

Configuring a VLAN on an 802.1Q switch creates a static VLAN entry. The entry will always remain registered and will not time out. However, dynamic entries will time-out and their registrations will be removed from the member list if the end station A is removed. This ensures that, if switches are disconnected or if end stations are removed, the registered information remains accurate.

The end result is that the port egress list of a port is updated with information about VLANs that reside on that port, even if the actual station on the VLAN is several hops away.

Figure 10-1 Example of VLAN Propagation via GVRP



Purpose

To dynamically create VLANs across a switched network. The GVRP command set is used to display GVRP configuration information, the current global GVRP state setting, individual port settings (enable or disable) and timer settings. By default, GVRP is enabled globally on the device, but disabled on all ports.

Commands

For information about...	Refer to page...
show gvrp	10-22
show garp timer	10-22
set gvrp	10-23
clear gvrp	10-24
set garp timer	10-24
clear garp timer	10-25

show gvrp

Use this command to display GVRP configuration information.

Syntax

show gvrp [*port-string*]

Parameters

port-string	(Optional) Displays GVRP configuration information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, GVRP configuration information will be displayed for all ports and the device.

Mode

Switch command, read-only.

Example

This example shows how to display GVRP status for the device and for fw.2.1:

```
C3(su)->show gvrp ge.2.1
Global GVRP status is enabled.

Port Number    GVRP status
-----------    -----------
ge.2.1         disabled
```

show garp timer

Use this command to display GARP timer values for one or more ports.

Syntax

show garp timer [*port-string*]

Parameters

port-string	(Optional) Displays GARP timer information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, GARP timer information will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display GARP timer information on ports 1 through 10 in slot 1:

Note: For a functional description of the terms **join**, **leave**, and **leaveall timers**, refer to the standard IEEE 802.1Q documentation, which is not supplied with this device.

```
C3(su)->show garp timer ge.1.1-10
 Port based GARP Configuration: (Timer units are centiseconds)
 Port Number     Join        Leave     Leaveall
 -----------  ----------  ----------  ----------
 ge.1.1             20          60        1000
 ge.1.2             20          60        1000
 ge.1.3             20          60        1000
 ge.1.4             20          60        1000
 ge.1.5             20          60        1000
 ge.1.6             20          60        1000
 ge.1.7             20          60        1000
 ge.1.8             20          60        1000
 ge.1.9             20          60        1000
 ge.1.10            20          60        1000
```

Table 10-3 provides an explanation of the command output. For details on using the **set gvrp** command to enable or disable GVRP, refer to "set gvrp" on page 10-23. For details on using the **set garp timer** command to change default timer values, refer to "set garp timer" on page 10-24.

Table 10-3 show gvrp configuration Output Details

Output Field	What It Displays...
Port Number	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
Join	Join timer setting.
Leave	Leave timer setting.
Leaveall	Leavall timer setting.

set gvrp

Use this command to enable or disable GVRP globally on the device or on one or more ports.

Syntax

`set gvrp {enable | disable}` [*`port-string`*]

Parameters

disable | **enable**	Disables or enables GVRP on the device.
port-string	(Optional) Disables or enables GVRP on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, GVRP will be disabled or enabled for all ports.

Mode

Switch command, read-write.

Examples

This example shows how to enable GVRP globally on the device:

```
C3(su)->set gvrp enable
```

This example shows how to disable GVRP globally on the device:

```
C3(su)->set gvrp disable
```

This example shows how to enable GVRP on `ge.1.3`:

```
C3(su)->set gvrp enable ge.1.3
```

clear gvrp

Use this command to clear GVRP status or on one or more ports.

Syntax

`clear gvrp` [*`port-string`*]

Parameters

port-string	(Optional) Clears GVRP status on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, GVRP status will be cleared for all ports.

Mode

Switch command, read-write.

Example

This example shows how to clear GVRP status globally on the device:

```
C3(su)->clear gvrp
```

set garp timer

Use this command to adjust the values of the join, leave, and leaveall timers.

Syntax

`set garp timer` {[**`join`** *`timer-value`*] [**`leave`** *`timer-value`*] [**`leaveall`** *`timer-value`*]} *`port-string`*

Parameters

join timer-value	Sets the GARP join timer in centiseconds (Refer to 802.1Q standard.)
leave timer-value	Sets the GARP leave timer in centiseconds (Refer to 802.1Q standard.)

leaveall timer-value	Sets the GARP leaveall timer in centiseconds (Refer to 802.1Q standard.)
port-string	Specifies the port(s) on which to configure GARP timer settings. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Usage

The setting of these timers is critical and should only be changed by personnel familiar with the 802.1Q standards documentation, which is not supplied with this device.

Examples

This example shows how to set the GARP join timer value to 100 centiseconds for all ports:

```
C3(su)->set garp timer join 100 *.*.*
```

This example shows how to set the leave timer value to 300 centiseconds for all ports:

```
C3(su)->set garp timer leave 300 *.*.*
```

This example shows how to set the leaveall timer value to 20000 centiseconds for all ports:

```
C3(su)->set garp timer leaveall 20000 *.*.*
```

clear garp timer

Use this command to reset GARP timers back to default values.

Syntax

clear garp timer {[**join**] [**leave**] [**leaveall**]} *port-string*

Parameters

join	(Optional) Resets the join timer to 20 centiseconds.
leave	(Optional) Resets the leave timer to 60 centiseconds.
leaveall	(Optional) Resets the leaveall time to 1000 centiseconds.
port-string	Specifies the port or ports on which to reset the GARP timer(s).

Defaults

At least one optional parameter must be entered.

Mode

Switch command, read-write.

Example

The example shows how to reset the GARP leave timer to 60 centiseconds.

```
C3(su)->clear garp timer leave ge.1.1
```

11

Policy Classification Configuration

This chapter describes the Policy Classification set of commands and how to use them.

Note: An Enterasys Networks Feature Guide document containing an in-depth discussion of Policy configuration is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

Policy Classification Configuration Summary

SecureStack C3 devices support policy profile-based provisioning of network resources by allowing IT administrators to:

- Create, change or remove policy profiles based on business-specific use of network services.
- Permit or deny access to specific services by creating and assigning classification rules which map user profiles to protocol-based frame filtering policies configured for a particular VLAN or Class of Service (CoS).
- Assign or unassign ports to policy profiles so that only ports activated for a profile will be allowed to transmit frames accordingly.

Note: It is recommended that you use Enterasys Networks NMS Policy Manager as an alternative to CLI for configuring policy classification on the SecureStack C3 devices.

Configuring Policy Profiles

Purpose

To review, create, change and remove user profiles that relate to business-driven policies for managing network resources.

Note: B3, C3, and G3 devices support profile-based CoS traffic rate limiting only. Policy rules specifying CoS will only rate limit on D2, C2 and B2 devices, including when C2 and B2 devices are configured on mixed stacks containing B3 and C3 devices.

Commands

For information about...	Refer to page...
show policy profile	11-2
set policy profile	11-4
clear policy profile	11-5

show policy profile

Use this command to display policy profile information.

Syntax

show policy profile {**all** | *profile-index* [*consecutive-pids*] [**-verbose**]}

Parameters

all | *profile-index*	Displays policy information for all profile indexes or a specific profile index.
consecutive-pids	(Optional) Displays information for specified consecutive profile indexes.
-verbose	(Optional) Displays detailed information.

Defaults

If optional parameters are not specified, summary information will be displayed for the specified index or all indices.

Mode

Switch command, read-only.

Example

This example shows how to display policy information for profile 11:

```
C3(su)->show policy profile 11
Profile Index           : 11
Profile Name            : MacAuth1
Row Status              : active
Port VID Status         : Enable
Port VID Override       : 11
CoS                     : 0
```

```
CoS Status                : Disable
Egress Vlans              : none
Forbidden Vlans           : none
Untagged Vlans            : none
Rule Precedence           : 1-31
                          :MACSource(1),MACDest(2),Unknown(3),
                          :Unknown(4),Unknown(5),Unknown(6),
                          :Unknown(7),Unknown(8),Unknown(9),
                          :Unknown(10),Unknown(11),IPSource(12),
                          :IPDest(13),IPFrag(14),UDPSrcPort(15),
                          :UDPDestPort(16),TCPSrcPort(17),TCPDestPort(18),
                          :ICMPType(19),Unknown(20),IPTOS(21),
                          :IPProto(22),Unknown(23),Unknown(24),
                          :Ether(25),Unknown(26),VLANTag(27),
                          :Unknown(28),Unknown(29),Unknown(30),
                          :port(31)
Admin Profile Usage       : none
Oper Profile Usage        : none
Dynamic Profile Usage     : none
```

Table 11-1 provides an explanation of the command output.

Table 11-1 show policy profile Output Details

Output Field	What It Displays...
Profile Index	Number of the profile.
Profile Name	User-supplied name assigned to this policy profile.
Row Status	Whether or not the policy profile is enabled (**active**) or disabled.
Port VID Status	Whether or not PVID override is **enabled** or **disabled** for this profile. If all classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
Port VID Override	The PVID assigned to packets, if PVID override is enabled.
CoS	CoS priority value to assign to packets, if CoS override is enabled.
CoS Status	Whether or not Class of Service override is **enabled** or **disabled** for this profile. If all classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
Egress VLANs	VLAN(s) that ports to which the policy profile is assigned can use for tagged egress.
Forbidden VLANs	VLAN(s) forbidden to ports to which the policy profile is assigned.
Untagged VLANs	VLAN(s) that ports to which the policy profile is assigned can use for untagged egress.
Rule Precedence	Displays the precedence of types of rules.
Admin Profile Usage	Ports administratively assigned to use this policy profile.
Oper Profile Usage	Ports currently assigned to use this policy profile.
Dynamic Profile Usage	Port dynamically assigned to use this policy profile.

set policy profile

Use this command to create a policy profile entry.

Syntax

```
set policy profile profile-index [name name] [pvid-status {enable | disable}]
[pvid pvid] [cos-status {enable | disable}] [cos cos] [egress-vlans egress-
vlans][forbidden-vlans forbidden-vlans] [untagged-vlans untagged-vlans]
[precedence precedence-list] [append] [clear]
```

Parameters

profile-index	Specifies an index number for the policy profile. Valid values are **1** - **255**.
name *name*	(Optional) Specifies a name for the policy profile. This is a string from 1 to 64 characters.
pvid-status enable | **disable**	(Optional) Enables or disables PVID override for this profile. If all classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
pvid *pvid*	(Optional) Specifies the PVID to packets, if PVID override is enabled and invoked as default behavior.
cos-status enable | **disable**	(Optional) Enables or disables Class of Service override for this profile. If all classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.  **Note:** A maximum of 99 rules can be supported per policy profile for policy profiles that have cos-status enabled.
cos *cos*	(Optional) Specifies a CoS value to assign to packets, if CoS override is enabled and invoked as default behavior. Valid values are **0** to **7**.
egress-vlans *egress-vlans*	(Optional) Specifies that the port to which this policy profile is applied should be added to the egress list of the VLANs defined by *egress-vlans*. Packets will be formatted as tagged.
forbidden-vlans *forbidden-vlans*	(Optional) Specifies that the port to which this policy profile is applied should be added as forbidden to the egress list of the VLANs defined by *forbidden-vlans*. Packets from this port will not be allowed to participate in the listed VLANs.
untagged-vlans *untagged-vlans*	(Optional) Specifies that the port to which this policy profile is applied should be added to the egress list of the VLANs defined by *untagged-vlans*. Packets will be formatted as untagged.
append	(Optional) Appends this policy profile setting to settings previously specified for this policy profile by the **egress-vlans**,**forbidden-vlans**, or **untagged-vlans** parameters. If **append** is not used, previous VLAN settings are replaced.
clear	(Optional) Appends this policy profile setting from settings previously specified for this policy profile by the **egress-vlans**,**forbidden-vlans**, or **untagged-vlans** parameters.
precedence *precedence-list*	(Optional) Assigns a rule precedence to this profile. Lower values will be given higher precedence. For a list of values, refer to the **show policy profile** command output.

Defaults

If optional parameters are not specified, none will be applied.

Mode

Switch command, read-write.

Example

This example shows how to create a policy profile 1 named “netadmin” with PVID override enabled for PVID 10, and Class-of-Service override enabled for CoS 5. This profile can use VLAN 10 for untagged egress:

```
C3(su)->set policy profile 1 name netadmin pvid-status enable pvid 10 cos-status
enable cos 5 untagged-vlans 10
```

clear policy profile

Use this command to delete a policy profile entry.

Syntax

clear policy profile *profile-index*

Parameters

profile-index	Specifies the index number of the profile entry to be deleted. Valid values are **1** to **255**.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to delete policy profile 8:

```
C3(su)->clear policy profile 8
```

Configuring Classification Rules

Purpose

To review, create, assign, and unassign classification rules to policy profiles. This maps user profiles to protocol-based frame filtering policies.

Note: B3, C3, and G3 devices support profile-based CoS traffic rate limiting only. Policy rules specifying CoS will only rate limit on D2, C2 and B2 devices, including when C2 and B2 devices are configured on mixed stacks containing B3 and C3 devices.

Commands

show policy rule

Use this command to display policy classification rule information.

Syntax

show policy rule [**all** | **admin-profile** | *profile-index*] [**ether** |**ipproto** | **ipdestsocket** | **ipsourcesocket** | **iptos** | **macdest** | **macsource** | **tcpdestport** | **tcpsourceport** | **udpdestport** | **udpsourceport**] [*data*] [**mask** *mask*] [**port-string** *port-string*] [**rule-status** {**active** | **not-in-service** | **not-ready**}] [**storage-type** {**non-volatile** | **volatile**}] [**vlan** *vlan*] | [**drop** | **forward**] [**dynamic-pid** *dynamic-pid*] [**cos** *cos*] [**admin-pid** *admin-pid*] [**-verbose**] [**usage-list**] [**display-if-used**]

Parameters

all | **admin-profile** | *profile-index*	Displays policy classification rules for **all** profiles, the **admin-profile**, or for a specific profile index number. Valid values are **1** - **1023**.
ether	Displays Ethernet type II rules.
ipproto	Displays IP protocol field in IP packet rules.
ipdestsocket	Displays IP destination address rules.
ipsourcesocket	Displays IP source address rules.
iptos	Displays Type of Service rules.
macdest	Displays MAC destination address rules.
macsource	Displays MAC source address rules.
tcpdestport	Displays TCP destination port rules.

tcpsourceport	Displays TCP source port rules.
udpdestport	Displays UDP destination port rules.
udpsourceport	Displays UDP source port rules.
data	Displays rules for a predefined classifier. This value is dependent on the classification type entered. Refer to Table 11-3 for valid values for each classification type.
mask *mask*	(Optional) Displays rules for a specific data mask. Refer to Table 11-3 for valid values for each classification type and data value**.**
port-string *port-string*	(Optional) Displays rules related to a specific ingress port.
rule-status active | **not-in-service** | **not-ready**	(Optional) Displays rules related to a specific rules status.
storage-type non-volatile | **volatile**	(Optional) Displays rules configured for either non-volatile or volatile storage.
vlan *vlan*	(Optional) Displays rules for a specific VLAN ID.
drop | **forward**	Displays rules based on whether matching packets will be dropped or forwarded.
dynamic-pid *dynamic-pid*	Displays rules associated with a specific dynamic policy ID.
cos *cos*	(Optional) Displays rules for a Class-of-Service value. (Not supported on B3, C3, G3 devices.)
admin-pid *admin-pid*	Displays rules associated with a specific administrative policy ID [1..1023].
-verbose	(Optional) Displays detailed information.
usage-list	(Optional) If selected, each rule's usage-list shall be checked and shall display only those ports which have applied this rule.
display-if-used	(Optional) Displays rule(s) only if they are applied to at least one port.

Defaults

If **verbose** is not specified, summary information will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display policy classification information for Ethernet type 2 rules

```
C3(su)->show policy rule ether
|PID  |Rule Type   |Rule Data            |Mk|PortStr   |RS|ST|VLAN|CoS |U|
|02   |Ether       |2048  (0x0800)       |16|All       | A|NV|fwrd|    |?|
|02   |Ether       |2049  (0x0801)       |16|All       | A|NV|drop|    |?|
|02   |Ether       |2989  (0x0bad)       |16|All       | A|NV|drop|    |?|
|02   |Ether       |33079 (0x8137)       |16|All       | A|NV|drop|    |?|
```

This example shows how to display policy classification information for administrative rule 1

```
C3(su)->show policy rule admin-pid 1
|Admin|Rule Type   |Rule Data            |Mk|PortStr   |RS|ST|dPID|aPID|U|
```

```
|admin|Port        |ge.1.1              |16|ge.1.1    | A|NV|    |   1|?|
|admin|Port        |ge.1.2              |16|ge.1.2    | A|NV|    |   1|?|
|admin|Port        |ge.1.3              |16|ge.1.3    | A|NV|    |   1|?|
|admin|Port        |ge.1.4              |16|ge.1.4    | A|NV|    |   1|?|
|admin|Port        |ge.1.5              |16|ge.1.5    | A|NV|    |   1|?|
|admin|Port        |ge.1.6              |16|ge.1.6    | A|NV|    |   1|?|
|admin|Port        |ge.1.7              |16|ge.1.7    | A|NV|    |   1|?|
|admin|Port        |ge.1.8              |16|ge.1.8    | A|NV|    |   1|?|
|admin|Port        |ge.1.9              |16|ge.1.9    | A|NV|    |   1|?|
|admin|Port        |ge.1.10             |16|ge.1.10   | A|NV|    |   1|?|
|admin|Port        |ge.1.11             |16|ge.1.11   | A|NV|    |   1|?|
|admin|Port        |ge.1.12             |16|ge.1.12   | A|NV|    |   1|?|
```

Table 11-2 provides an explanation of the command output.

Table 11-2 show policy rule Output Details

Output Field	What It Displays...
PID	Profile index number. Assigned to this classification rule with the **set policy profile** command (“set policy profile” on page 11-4).
Rule Type	Type of classification rule. Refer to Table 11-3 for valid types.
Rule Data	Rule data value. Refer to Table 11-3 for valid values for each classification type.
Mk	Rule data mask. Refer to Table 11-3 for valid values for each classification data value.
PortStr	Ingress port(s) to which this rule applies.
RS	Whether or not the status of this rule is active (A), not in service or not ready.
ST	Whether or not this rule’s storage type is non-volatile (NV) or volatile (V).
VLAN	VLAN ID to which this rule applies and whether or not matching packets will be dropped or forwarded.
CoS	If applicable, Class of Service value to which this rule applies.
U	Whether or not this rule has been used.
dPID	Whether or not this is a dynamic profile ID.
aPID	Whether or not this is an administrative profile ID.

show policy capability

Use this command to display detailed policy classification capabilities supported by your SecureStack C3 device.

Syntax

`show policy capability`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Usage

Use this command to display detailed policy classification capabilities supported by your SecureStack C3 device. The output of this command shows a table listing classifiable traffic attributes and the type of actions, by rule type, that can be executed relative to each attribute. Above the table is a list of all the actions possible on this device.

The left-most column of the table lists all possible classifiable traffic attributes. The next two columns from the left indicate how policy profiles may be assigned, either administratively or dynamically. The next four columns from the left indicate the actions that may be performed. The last three columns indicate auditing options.

An x in an action column for a traffic attribute row indicates that your system has the capability to perform that action for traffic classified by that attribute.

Example

This example shows how to display the device's policy classification capabilities. Refer to "set policy rule" on page 11-10 for a description of the parameters displayed:

```
C3(su)->show policy capability

The following supports related to policy are supported in this device:
VLAN Forwarding              Priority                      Permit
Deny                         Precedence Reordering         Rules Table
Longest Prefix Rules
 ============================================================
|                          | D |   |   |   | F |   |   | D |
|                          | Y |   |   |   | O | S |   | I |
|                          | N | A |   |   | R | Y |   | S |
|                          | A | D | V |   | D | W | S | T | A |
|                          | M | M | L | C | R | A | L | R | B |
|                          | I | I | A | O | O | R | O | A | L |
| SUPPORTED RULE TYPES     | C | N | N | S | P | D | G | P | E |
 ============================================================
|MAC source address        |   |   |   | X | X | X |   |   |   |
|MAC destination address   |   |   |   | X | X | X |   |   |   |
|IPX source address        |   |   |   |   |   |   |   |   |   |
|IPX destination address   |   |   |   |   |   |   |   |   |   |
|IPX source socket         |   |   |   |   |   |   |   |   |   |
|IPX destination socket    |   |   |   |   |   |   |   |   |   |
|IPX transmission control  |   |   |   |   |   |   |   |   |   |
|IPX type field            |   |   |   |   |   |   |   |   |   |
|IPv6 source address       |   |   |   |   |   |   |   |   |   |
|IPv6 destination address  |   |   |   |   |   |   |   |   |   |
|IPv6 flow label           |   |   |   |   |   |   |   |   |   |
|IP source address         |   |   |   | X | X | X |   |   |   |
|IP destination address    |   |   |   | X | X | X |   |   |   |
|IP fragmentation          |   |   |   |   |   |   |   |   |   |
|UDP port source           |   |   |   | X | X | X |   |   |   |
|UDP port destination      |   |   |   | X | X | X |   |   |   |
|TCP port source           |   |   |   | X | X | X |   |   |   |
|TCP port destination      |   |   |   | X | X | X |   |   |   |
|ICMP packet type          |   |   |   |   |   |   |   |   |   |
|TTL                       |   |   |   |   |   |   |   |   |   |
|IP type of service        |   |   |   | X | X | X |   |   |   |
|IP proto                  |   |   |   | X | X | X |   |   |   |
```

```
|Ether II packet type     |   |   | X | X | X | X |   |   |   |
|LLC DSAP/SSAP/CTRL       |   |   |   |   |   |   |   |   |   |
|VLAN tag                 |   |   |   |   |   |   |   |   |   |
|Replace tci              |   |   |   |   |   |   |   |   |   |
|Port string              | X | X | X | X | X | X |   |   |   |
=============================================================
```

set policy rule

Use this command to assign incoming untagged frames to a specific policy profile and to VLAN or Class-of-Service classification rules.

Note: Refer to Appendix A, **Policy and Authentication Capacities** for information about limits on certain rule types for this platform.

Syntax

This command has two forms of syntax—one to create an admin rule, and the other to create a traffic classification rule and attach it to a policy profile.

set policy rule admin-profile {**vlantag** *data* [**mask** *mask*] **admin-pid** *profile-index*} [**port-string** *port-string*]

set policy rule *profile-index* {**ether** | **ipproto** | **ipdestsocket** | **ipsourcesocket** | **iptos** | **macdest** | **macsource** | **tcpdestport** | **tcpsourceport** | **udpdestport** | **udpsourceport**} *data* [**mask** *mask*] {[**vlan** *vlan*] [**cos** *cos*] | [**drop** | **forward**]}

Note: Classification rules are automatically enabled when created.

Parameters

The following parameters apply to creating an admin rule. See the Usage section below for more information about admin rules.

admin-profile	Specifies that this is an admin rule.
vlantag *data*	Classifies based on VLAN tag specified by *data*. Value of *data* can range from 1 to 4094 or 0xFFF.
mask *mask*	(Optional) Specifies the number of significant bits to match, dependent on the *data* value entered. Value of *mask* can range from 1 to 12. Refer to Table 11-3 for valid values for each classification type and data value**.**
admin-pid *profile-index*	Associates this admin rule with a policy profile, identified by its index number. Policy profiles are configured with the **set policy profile** command as described in "set policy profile" on page 11-4. Valid *profile-index* values are **1**- **255**.
port-string *port-string*	(Optional) Assigns this rule with the specified policy profile on specific ingress port(s). Rule would not be used until policy is assigned to the specified port(s) using the **set policy port** command as described in "set policy port" on page 11-15.

The following parameters apply to creating a traffic classification rule.

profile-index	Specifies a policy profile number to which this rule will be assigned. Policy profiles are configured with the **set policy profile** command as described in "set policy profile" on page 11-4. Valid *profile-index* values are **1- 255**.
ether	Specifies that the rule should apply to traffic with the specified type field in Ethernet II packet.
ipproto	Specifies that the rule should apply to traffic with the specified Protocol field in IP packet.
ipdestsocket	Specifies that the rule should apply to traffic with the specified destination IP address with optional post-fixed port.
ipsourcesocket	Specifies that the rule should apply to traffic with the specified source IP address, with optional post-fixed port.
iptos	Specifies that the rule should apply to traffic with the specified Type of Service field in IP packet.
macdest	Specifies that the rule should apply to traffic with the specified MAC destination address.
macsource	Specifies that the rule should apply to traffic with the specified MAC source address.
tcpdestport	Specifies that the rule should apply to traffic with the specified TCP destination port.
tcpsourceport	Specifies that the rule should apply to traffic with the specified TCP source port.
udpdestport	Specifies that the rule should apply to traffic with the specified UDP destination port.
udpsourceport	Specifies that the rule should apply to traffic with the specified UDP source port.
data	Specifies the code for the specified traffic classifier (listed above). This value is dependent on the classification type entered. Refer to Table 11-3 for valid values for each classification type.
mask *mask*	(Optional) Specifies the number of significant bits to match, dependent on the *data* value entered. Refer to Table 11-3 for valid values for each classification type and data value**.**
vlan *vlan*	Specifies the action of the rule is to classify to a VLAN ID.
cos *cos*	Specifies the action of the rule is to classify to a Class-of-Service ID. Valid values are **0 - 4095**. A value of -1 indicates that no CoS forwarding behavior modification is desired. (Not supported on B3, C3, and G3.)
drop | **forward**	Specifies that packets within this classification will be dropped or forwarded.

Defaults

None.

Mode

Switch command, read-write.

Usage

An admin rule can be used to map incoming tagged frames to a policy role (profile). There can be only one admin rule configured per system (stack). Typically, this rule is used to implement the "User + IP phone" legacy feature. Refer to "Configuring User + IP Phone Authentication" on page 26-48 for more information. You would configure a policy profile/role for IP phones (for example, assigning the traffic to a "voice" VLAN), then associate that policy profile with the admin rule, and associate the admin rule with the desired ports. Users authenticating over the same port will typically use a dynamically assigned policy role.

A policy classification rule has two main parts: Traffic Description and Actions. The Traffic Description identifies the type of traffic to which the rule will pertain. Actions specify whether that traffic will be assigned class of service, assigned to a VLAN, or both.

Table 11-3 provides the **set policy rule** *data* values that can be entered for a particular parameter, and the *mask* bits that can be entered for each classifier associated with that parameter.

Table 11-3 Valid Values for Policy Classification Rules

Classification Rule Parameter	*data* value	*mask* bits
ether	Type field in Ethernet II packet: **1536** - **65535** or **0x600 - 0xFFFF**	Not applicable.
ipproto	Protocol field in IP packet: **0 - 255** or **0 - 0xFF**	Not applicable.
Destination or Source IP Address: ipdestsocket ipsourcesocket	IP Address in dotted decimal format: **000.000.000.000** and (Optional) post-fixed port: **0** - **65535**	**1** - **48**
iptos	Type of Service field in IP packet: **0 - 252** or **0 - 0xFC**	Not applicable.
Destination or Source MAC: macdest macsource	MAC Address: **00-00-00-00-00-00**	**1** - **48**
Destination or Source TCP port: tcpdestport tcpsourceport	TCP Port Number: **0 - 65535** or **0 - 0xFFFF**	**1** - **16**
Destination or Source UDP port: udpsourceport udpdestport	UDP Port Number: **0 - 65535** or **0 - 0xFFFF**	**1** - **16**
vlantag	VLAN tag: **1**- **4094**	Not applicable.

Examples

This example shows how to use Table 11-3 to assign a rule to policy profile 3 that will filter Ethernet II Type 1526 frames to VLAN 7:

```
C3(su)->set policy rule 3 ether 1526 vlan 7
```

This example shows how to use Table 11-3 to assign a rule to policy profile 5 that will forward UDP packets from source port 45:

```
C3(su)->set policy rule 5 udpportsource 45 forward
```

This example shows how to use Table 11-3 to assign a rule to policy profile 1 that will drop IP source traffic from IP address 1.2.3.4. If mask 32 is not specified as shown, a default mask of 48 bits (IP address + port) would be applied:

```
C3(su)->set policy rule 1 ipsourcesocket 1.2.3.4 mask 32 drop
```

clear policy rule

Use this command to delete policy classification rule entries.

Syntax

This command has two forms of syntax—one to clear an admin rule (for policy ID 0), and the other to clear a classification rule.

clear policy rule admin-profile {**vlantag** *data* [**mask** *mask*]

clear policy rule *profile-index* {**all-pid-entries** | {**ether** | **ipproto** | **ipdestsocket** | **ipsourcesocket** | **iptos** | **macdest** | **macsource** | **tcpdestport** | **tcpsourceport** | **udpdestport** | **udpsourceport**}}

Parameters

The following parameters apply to deleting an admin rule.

admin-profile	Specifies that the rule to be deleted is an admin rule for policy ID 0.
vlantag *data*	Deletes the rule based on VLAN tag specified by *data*. Value of *data* can range from 1 to 4094 or 0xFFF.
mask *mask*	(Optional) Specifies the number of significant bits to match, dependent on the *data* value entered. Value of *mask* can range from 1 to 12. Refer to Table 11-3 for valid values for each classification type and data value**.**

The following parameters apply to deleting a classification rule.

profile-index	Specifies a policy profile for which to delete classification rules. Valid *profile-index* values are **1** - **255**.
all-pid-entries	Deletes all entries associated with the specified policy profile.
ether	Deletes associated Ethernet II classification rule.
ipproto	Deletes associated IP protocol classification rule.
ipdestsocket	Deletes associated IP destination classification rule.
ipsourcesocket	Deletes associated IP source classification rule.
iptos	Deletes associated IP Type of Service classification rule.
macdest	Deletes associated MAC destination address classification rule.
macsource	Deletes associated MAC source address classification rule.
tcpdestport	Deletes associated TCP destination port classification rule.
tcpsourceport	Deletes associated TCP source port classification rule.
udpdestport	Deletes associated UDP destination port classification rule.
udpsourceport	Deletes associated UDP source port classification rule.

Defaults

When applicable, *data* and *mask* must be specified for individual rules to be cleared.

Mode

Switch command, read-write.

Examples

This example shows how to delete Ethernet II Type 1526 classification rule entries associated with policy profile 1 from all ports.

```
C3(su)->clear policy rule 1 ether 1526
```

This example shows how to remove a rule from policy profile 5 that will forward UDP frames from source port 45.

```
C3(su)->clear policy rule 5 udpportsource 45 forward
```

clear policy all-rules

Use this command to remove all policy classification rules.

Syntax

`clear policy all-rules`

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to remove all administrative and policy index rules:

```
C3(su)->clear policy all-rules
```

Assigning Ports to Policy Profiles

Note: Refer to Appendix A, **Policy and Authentication Capacities** for information about policy limits for this platform.

Purpose

To assign and unassign ports to policy profiles.

Commands

For information about...	Refer to page...
set policy port	11-15
clear policy port	11-16

set policy port

Use this command to assign ports to a policy profile.

Syntax

`set policy port` *`port-string profile-index`*

Parameters

port-string	Specifies the port(s) to add to the policy profile. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
profile-index	Specifies the ID of the policy profile (role) to which the port(s) will be added. This value must match the *profile-index* value assigned using the **set policy profile** command ("set policy profile" on page 11-4) in order for a policy profile to be active on the specified port.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to allow Gigabit Ethernet ports 5 through 15 in slot 1 to transmit frames according to policy profile 1:

```
C3(su)->set policy port ge.1.5-15 1
```

clear policy port

Use this command to remove a policy profile from one or more ports.

Syntax

clear policy port *port-string profile-index*

Parameters

port-string	Specifies the port(s) from which to remove the policy profile. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
profile-index	Specifies the ID of the policy profile (role) to which the port(s) will be added. This value must match the *profile-index* value assigned using the **set policy profile** command ("set policy profile" on page 11-4) in order for a policy profile to be active on the specified port.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to remove policy profile 10 from port 21 in slot 1:

```
C3(rw)->clear policy port ge.1.21 10
```

Configuring Policy Class of Service (CoS)

Note: It is recommended that you use Enterasys Networks NMS Policy Manager as an alternative to CLI for configuring policy-based CoS on the switches.

The SecureStack C3 supports Class of Service (CoS), which allows you to assign mission-critical data to a higher priority through the device by delaying less critical traffic during periods of congestion. The higher priority traffic going through the device is serviced first (before lower priority traffic). The Class of Service capability of the device is implemented by a priority queueing mechanism. Class of Service is based on the IEEE 802.1D (802.1p) standard specification, and allows you to define eight priorities (0-7, with 7 granted highest priority) and up to 8 transmit queues (0-7) for each port.

By default, policy-based CoS is disabled on the device, and default or user-assigned port-based 802.1D (802.1p) settings are used to determine traffic prioritization. When policy-based CoS is enabled, the default and user-assigned policy-based settings will override port-based settings described in Chapter 12.

Class of Service functionality can also be used to control broadcast, unknown unicast, and/or multicast flooding. This feature prevents configured ports from being disrupted by a traffic storm by rate-limiting specific types of packets through those ports. Refer to "About CoS-Based Flood Control" on page 11-19 for more information.

About Policy-Based CoS Configurations

Once enabled using the **set cos state** command, you can add to the policy-based CoS function by defining new port groupings, and assigning inbound rate limiters. The process for user-defined CoS configuration involves the following steps and associated commands listed in Procedure 11-1. An example follows the procedure.

Procedure 11-1 User-Defined CoS Configuration

Step	Task	Command(s)
1.	Enable CoS	**set cos state enable**
2.	Create CoS IRL port groups	**set cos port-config irl**
3.	Define physical rate limiters for groups	**set cos port-resource irl**
4.	Create virtual reference for the IRL resource (physical reference) for each port group	**set cos reference**
5.	Add IRL reference to CoS settings table	**set cos settings**

Example

This example creates different inbound rate limiters for two port groups and then assigns them to traffic with a CoS setting of 0.

1. Configure two port groups, one for user ports and one for uplink ports and assign ports to the groups. Port group 1.0 will represent user ports, group 2.0 will represent uplink ports.

```
C3(su)->set cos port-config irl 1.0 name Users ports ge.1.1-46
C3(su)->set cos port-config irl 2.0 name Uplink ports ge.1.47-48

C3(su)->show cos port-config
Inbound Rate Limiting Port Configuration Entries
```

```
------------------------------------------------------------------------
Port Group Name  :Default
Port Group       :0
Port Type        :0
Assigned Ports   :none
------------------------------------------------------------------------
Port Group Name  :Users
Port Group       :1
Port Type        :0
Assigned Ports   :ge.1.1-46
------------------------------------------------------------------------
Port Group Name  :Uplink
Port Group       :2
Port Type        :0
Assigned Ports   :ge.1.47-48
------------------------------------------------------------------------
```

2. Configure physical inbound rate limiters for each port group. For the user port group (1.0), create an IRL (irl-index of 1) for 512 kbps. For the uplink port group (2.0), create an IRL (irl-index of 1) for 10 megabits per second (10,000 kbps).

```
C3(su)->set cos port-resource irl 1.0 1 unit kbps rate 512
C3(su)->set cos port-resource irl 2.0 1 unit kbps rate 10000

C3(su)->show cos port-resource irl 1.0 1
Group Index Resource Type Unit    Rate      Rate Limit Type Action
----------- -------- ---- ---- ----------   --------------- ------
1.0         1        irl  kbps 512          drop            none

C3(su)->show cos  port-resource irl 2.0 1
Group Index Resource Type Unit    Rate      Rate Limit Type Action
----------- -------- ---- ---- ----------   --------------- ------
2.0         1        irl  kbps 10000        drop            none
```

3. In the CoS IRL reference mapping table for each port group, create a reference for each IRL resource created in the previous step. We will use reference number 1.

```
C3(su)->set cos reference irl 1.0 1 rate-limit 1
C3(su)->set cos reference irl 2.0 1 rate-limit 1

C3(su)->show cos reference irl 1.0

Group Index Reference Type Rate Limiter
----------- --------- ---- ------------
1.0         0         irl  none
1.0         1         irl  1
1.0         2         irl  none
1.0         3         irl  none
...
1.0         97        irl  none
1.0         98        irl  none
1.0         99        irl  none

C3(su)->show cos reference irl 2.0

Group Index Reference Type Rate Limiter
----------- --------- ---- ------------
2.0         0         irl  none
2.0         1         irl  1
2.0         2         irl  none
2.0         3         irl  none
...
```

```
2.0         97         irl  none
2.0         98         irl  none
2.0         99         irl  none
```

4. In the CoS settings table, configure a CoS setting for CoS index 1, which has a priority of 0. We enter the IRL reference, created in the previous step.

```
C3(su)->set cos settings 0 irl-reference 1
C3(su)->show cos settings
CoS Index Priority   ToS     IRL
--------- ---------- ------- -----
   0         0          *       1
   1         1          *       *
   2         2          *       *
   3         3          *       *
   4         4          *       *
   5         5          *       *
   6         6          *       *
   7         7          *       *
```

About CoS-Based Flood Control

Note: CoS-based flood control does not require a policy license on SecureStack B3 switches or on standalone D2 switches.

CoS-based flood control prevents configured ports from being disrupted by a traffic storm by rate-limiting specific types of packets through those ports. When flood control is enabled on a port, incoming traffic is monitored over one second intervals. During an interval, the incoming traffic rate for each configured traffic type (unicast, broadcast, multicast) is compared with the configured traffic flood control rate, specified in packets per second.

If, during a one second interval, the incoming traffic of a configured type reaches the traffic flood control rate configured on the port, CoS-based flood control drops the traffic until the interval ends. Packets are then allowed to flow again until the limit is again reached.

The following procedure describes the steps and commands required to configure CoS-based flood control.

Procedure 11-2

Step	Task	Command(s)
1.	Enable CoS.	**set cos state enable**
2.	Create a CoS flood control port resource, which specifies flood control rate limiters that can be mapped to specific ports.	**set cos port-resource flood-ctrl**
3.	Assign the flood control resource to specific ports.	**set cos port-config flood-ctrl**

Example

This example creates a broadcast rate limiter (index 1.0) of 5 packets per second and assigns it to ports ge.1.2 and ge.2.2.

```
C3(su)->set cos state enable
C3(su)->set cos port-resource flood-ctrl 1.0 broadcast rate 5
C3(su)->set cos port-config flood-ctrl 1.0 ports ge.1.2;ge.2.2 append
```

Commands

set cos state

Use this command to enable or disable Class of Service.

Syntax

```
set cos state {enable | disable}
```

Parameters

enable | disable	Enables or disables Class of Service on the switch. Default state is disabled.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to enable Class of Service:

```
C3(rw)->set cos state enable
```

show cos state

Use this command to display the Class of Service enable state.

Syntax

```
show cos state
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to show the Class of Service enable state:

```
C3(rw)->show cos state
Class-of-Service application is enabled
```

clear cos state

Use this command to set CoS state back to its default setting of disabled.

Syntax

```
clear cos state
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the CoS state back to its default setting of disabled:

```
C3(su)->clear cos state
```

set cos settings

Use this command to configure a Class of Service entry in the CoS settings table.

Syntax

set cos settings *cos-index* **priority** *priority* [**tos-value** *tos-value*] [**irl-reference** *irl-reference*]

Parameters

cos-index	Specifies a Class of Service entry. Valid values are **0** to **255**.
priority *priority*	Specifies an 802.1d priority value. Valid values are **0** to **7**, with 0 being the lowest priority. See Usage section below for more information.
tos-value *tos-value*	(Optional) Specifies a Type of Service value. Valid values are **0** to **255**. See Usage section below for more information.
irl-reference *irl-reference*	(Optional) Set the inbound rate limiter associated with this entry. Valid values are 0 to 99. See Usage section below for more information.

Defaults

If no optional parameters are specified, none will be applied.

Mode

Switch command, read-write.

Usage

The CoS settings table takes individual class of service features and displays them as belonging to a CoS entry. Essentially, it is used for CoS feature assignment. Each class of service entry consists of an index, 802.1p priority, an optional ToS value, and an IRL reference.

- **CoS Index**

  Indexes are unique identifiers for each CoS setting. CoS indexes 0 through 7 are created by default and mapped directly to 802.1p priority for backwards compatibility. These entries cannot be removed, and 802.1p priority values cannot be changed. When CoS is enabled, indexes are assigned. Up to 256 CoS indexes or entries can be configured.

- **Priority**

  802.1p priority can be applied per CoS index. For each new CoS index created, the user has the option to assign an 802.1p priority value 0 to 7 for the class of service. CoS indexes 0 through 7 map directly to 802.1p priorities and cannot be changed as they exist for backward compatibility.

- **ToS**

  This value can be set per class of service, but is not required. When a frame is assigned to a class of service for which this value is configured, the ToS field of the incoming IP packet will be overwritten to the user-defined value. All but the last two bits of the ToS field are rewritable. ToS can be set for CoS indexes 0 through 7.

- **IRL Reference**

  The CoS IRL reference field is optional, as rate limits are not required. The IRL reference does not assign an inbound rate limit but points to the CoS IRL Reference Mapping Table. This reference may be thought of as the virtual rate limiter that will assign the physical rate limiter defined by the IRL Reference Mapping Table.

Example

This example shows how to create CoS entry 8 with a priority value of 3:

```
C3(rw)->set cos settings 8 priority 3
```

clear cos settings

Use this command to clear Class of Service entry settings.

Syntax

clear cos settings *cos-list* {[**all**] | [**priority**] [**tos-value**] [**irl-reference**]}

Parameters

cos-list	Specifies a Class of Service entry to clear.
all	Clears all settings associated with this entry.
priority	Clears the priority value associated with this entry.
tos-value	Clears the Type of Service value associated with this entry.
irl-reference	Clear the IRL reference associated with this entry.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the priority for CoS entry 8:

```
C3(rw)->clear cos settings 8 priority
```

show cos settings

Use this command to display Class of Service parameters.

Syntax

show cos settings [*cos-list*]

Parameters

cos-list	(Optional) Specifies a Class of Service entry to display.

Defaults

If not specified, all CoS entries will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to show all CoS settings:

```
C3(su)->show cos settings
CoS Index Priority   ToS     IRL       flood-ctrl
--------- ---------- ------- -------   ----------
   0         0          48      *          enabled
   1         1          *       *          enabled
   2         2          *       *          enabled
   3         3          *       *          enabled
   4         4          *       *          enabled
   5         5          *       *          enabled
   6         6          *       *          enabled
   7         7          *       *          enabled
```

set cos port-config

Use this command to create a port group for inbound rate limiting or flood control and add or remove ports from the group.

Syntax

set cos port-config {**irl**|**flood-ctrl**} *group-type-index* [**name** *name*] [**ports** *port-list*] [**append**] | [**clear**]

Parameters

irl	Specifies that this is an inbound rate limiting (IRL) port group.
flood-ctrl	Specifies that this is a flood control port group.
group-type-index	Specifies an inbound rate limiting port group/type index. Valid entries are in the form of **group#.port-type**. Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as **3.0**.
name *name*	(Optional) User defined name for the **group**.
ports *port-list*	(Optional) Ports assigned to the **group**. All ports must be of the same port **type** (Fast Ethernet, Gigabit Ethernet).
append	(Optional) Append (add) the ports to the ports that are already in the **group**.
clear	(Optional) Clear the given ports from those assigned to the **group**.

Defaults

None.

Mode

Switch command, read-write.

Usage

CoS port groups are identified by group number and the type of ports in the group, in the form of **group#.port-type**. The port group 0.0 exists by default. This default port group cannot be removed and all physical ports in the system are assigned to it. Up to seven additional port groups (1

through 7) can be configured. Currently, only one port type (type 0) is supported. This port type supports 100 limiters.

Additional port groups may be created for flexibility. Ports assigned to a new port group must be mutually exclusive from the other port group entries—ports are automatically removed from the default port group—and must be comprised of the same port type as defined by the port group.

The creation of additional port groups could be used to combine similar ports by their function for flexibility. For instance, ports associated to users can be added to a port group called “Users” and ports associated to uplink ports can be added to a port group called “Uplink.” Using these port groups, a single class of service can assign different rate limits to each port group. “User” ports can be assigned one rate limit, while “Uplink” ports can be assigned another.

The command show cos port-config displays each port group configured by group and type, with the group name and associated (assigned) ports. The command show cos port-type displays the available inbound rate limiting resources for the port type.

Example

This example configures two port groups, one for user ports and one for uplink ports and assign ports to the groups. Port group 1.0 will represent user ports, group 2.0 will represent uplink ports.

```
C3(su)->set cos port-config irl 1.0 name Users ports ge.1.1-46
C3(su)->set cos port-config irl 2.0 name Uplink ports ge.1.47-48
```

show cos port-config

Use this command to show CoS port groups and the assigned ports.

Syntax

show cos port-config [**irl**|**flood-ctrl** [*group-type-index*]]

Parameters

irl	(Optional) Specifies that inbound rate limiting configuration information should be displayed.
flood-ctrl	(Optional) Specifies that flood control rate configuration information should be displayed.
group-type-index	(Optional) Show assigned ports for a specific port group. Valid entries are in the form of **group#.port-type**. Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as **3.0**.

Defaults

The **show cos port-config** command by itself will show all Port Groups.

Mode

Switch command, read-only.

Example

This example shows all inbound rate limiting port groups. Note that ports ge.1.1 through ge.1.48 were removed from the default port group 0.0 when they were added to port groups 1.0 and 2.0.

```
C3(su)->show cos port-config irl

Inbound Rate Limiting Port Configuration Entries
--------------------------------------------------------------------------
Port Group Name  :Default
Port Group       :0
Port Type        :0
Assigned Ports   :none
--------------------------------------------------------------------------
Port Group Name  :Users
Port Group       :1
Port Type        :0
Assigned Ports   :ge.1.1-46
--------------------------------------------------------------------------
Port Group Name  :Uplink
Port Group       :2
Port Type        :0
Assigned Ports   :ge.1.47-48
--------------------------------------------------------------------------
```

clear cos port-config

Use this command to clear CoS port groups or assigned ports.

Syntax

clear cos port-config {**irl**|**flood-ctrl**} {**all** | *group-type-index* [**entry**] | [**name**] [**ports**]}

Parameters

irl	Clear an IRL port group configuration.
flood-ctrl	Clear a flood control port group configuration.
all	Clear all inbound rate limiting port-config non-default entries.
group-type-index	Delete a specific port group or group name, or clear the ports from that group. Valid entries are in the form of **group#.port-type**. Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as **3.0**.
entry	Delete this non-default inbound rate limiter entry.
name	Clear the administratively assigned textual description of this port group entry to its default.
ports	Clear the ports assigned to this group to its default.

Defaults

None.

Mode

Switch command, read-write.

Usage

The default port group 0.0 cannot be deleted.

Example

This example deletes all IRL Port Groups except for the Default group 0.0:

```
C3(su)->clear cos port-config irl all
```

set cos port-resource irl

Use this command to set the inbound rate limit parameters for a specific IRL resource for a specific port group.

Syntax

set cos port-resource irl *group-type-index irl-index* {[**unit** {**kbps**}] [**rate** *rate*] [**type** {**drop**}]}[**syslog enable** | **disable**] [**trap enable**|**disable**]

Parameters

group-type-index	Specifies an inbound rate limiting port group/type index. Valid entries are in the form of **group#.port-type**. Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as **3.0**.
irl-index	Index number of the inbound rate limiter resource associated with this entry. Valid values range from 0 to 99.
unit	Unit of measure for the inbound rate limiter (only option is Kbps).
kbps	Kilobits per second.
rate *rate*	Data rate for this inbound rate limiter. This is the actual rate limit. Valid values range from 512 to 1,000,000 Kbps for a Gigabit port.
type drop	Action for the rate limiter. The only action option is drop the frame if all limiters are exceeded.
syslog enable|**disable**	Enable or disable reporting a syslog entry if limiters are exceeded.
trap enable|**disable**	Enable or disable sending a trap if limiters are exceeded.

Defaults

None.

Mode

Switch command, read-write.

Usage

CoS port resources are where actual physical rate limiters are configured. Resources map directly to the number of rate limiters supported by the port type. (Port type 0 supports 100 IRL resources.) Resources exist for each port group and are indexed as **group#.port-type.irl-index**. Port resources are not initially configured as rate limiting.

Inbound rate limiting, or rate policing, simply drops or clips traffic inbound if a configured rate is exceeded. CoS inbound rate limiting allows the user to configure rate limits based on kilobits per second.

The show cos port-resource command displays the resources available for each port group. By default, no IRL resources are configured. The default Rate Limiting algorithm is drop and cannot be configured otherwise.

Example

This example sets the inbound rate limit resource index number 1 for port group 2.0 to 10000 Kbps or 1 MB:

```
C3(su)->set cos port-resource irl 2.0 1 unit kbps rate 10000 type drop
```

set cos port-resource flood-ctrl

Use this command to create a CoS-based flood control port resource. This resource specifies flood control rate limiters that can be mapped to specific ports.

Syntax

set cos port-resource flood-ctrl *group-type-index* {**unicast** | **multicast** | **broadcast** | **all**} **rate** *rate*

Parameters

group-type-index	Specifies a port group/type index. Valid entries are in the form of **group#.port-type**. Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as **3.0**.
unicast	Specifies rate limiting will be applied to unknown unicast traffic.
multicast	Specifies rate limiting will be applied to multicast traffic.
broadcast	Specifies rate limiting will be applied to broadcast traffic.
all	Specifies rate limiting will be applied to unknown unicast, multicast, and broadcast traffic.
rate *rate*	Specifies a rate limit in packets per second.

Defaults

None.

Mode

Switch command, read-write.

Usage

CoS port resources are where actual physical rate limiters are configured. This command can be used to create up to three different flood control limit resources for the port-type index of 0. The resources are assigned to specific ports with the **set cos port-config** command.

Example

This example creates a port resource broadcast rate limiter of 5 packets per second for the port group type index of 1.0 (group # 1 of port-type index 0).

```
C3(su)->set cos port-resource flood-ctrl 1.0 broadcast rate 5
```

show cos port-resource

Use this command to display the configured port resources.

Syntax

show cos port-resource [**irl** [*group-type-index* [*irl-index*]]] | [**flood-ctrl** [*group-type-index*]]

Parameters

irl	(Optional) Specifies that inbound rate limiting port resources should be displayed.
flood-ctrl	(Optional) Specifies that flood control port resources should be displayed.
group-type-index	(Optional) Specifies a port group/type index. Valid entries are in the form of **group#.port-type**. Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as **3.0**.
irl-index	(Optional) Inbound rate limiter resource index configured for the specified port group. Valid values range from 0 to 99.

Defaults

If **irl** or **flood-ctrl** are not specified, all port resources are shown.

If a port group and IRL index are not specified, the IRL configuration for all resources (0-99) for all configured port groups will be shown.

If a port group is not specified with the **flood-ctrl** parameter, flood control resources for all configured port groups will be shown.

Mode

Switch command, read-only.

Examples

This example displays the IRL resource index number 1 configuration for group 2.0.

```
C3(su)->show cos port-resource irl 2.0 1

'?' after the rate value indicates an invalid rate value

Group Index Resource Type Unit    Rate      Rate Limit Type Action
```

```
----------- -------- ---- ---- ----------   --------------- ------
2.0         1        irl  kbps 10000        drop            none
```

This example displays the flood control resources configured for group 1.0.

```
C3(su)->show cos port-resource flood-ctrl 1.0

'?' after the rate value indicates an invalid rate value

Group      Resource       Type       Unit     Rate       Rate Limit       Action
Index                                                      type
---------  -----------   ----------   ----   ----------  ---------------  ------
1.0        ucast        flood-ctrl    pps     20         drop             none
1.0        mcast        flood-ctrl    pps     10         drop             none
1.0        bcast        flood-ctrl    pps     5          drop             none
```

clear cos port-resource irl

Use this command to clear inbound rate limit resources to default values.

Syntax

clear cos port-resource irl {**all** | *group-type-index* [*irl-index* [**unit**] [**rate**] [**type**]]}

Parameters

all	Clear all IRL resources for all port groups.
group-type-index	Specifies an inbound rate limiting port group/type index. Valid entries are in the form of **group#.port-type**. Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as **3.0**.
irl-index	(Optional) Inbound rate limiter resource index associated with the specified port group. Valid values range from 0 to 99.
unit	Clear the unit of measure for the inbound rate limiter.
rate	Clear the data rate for this inbound rate limiter.
type	Clear the action for the rate limiter.

Defaults

None.

Mode

Switch command, read-write.

Example

This example clears the data rate to 0 for IRL resource index 1 for group 2.0.

```
C3(su)->clear cos port-resource irl 2.0 1 rate
```

clear cos port-resource flood-ctrl

Use this command to clear flood control port resources to default values.

Syntax

clear cos port-resource flood-ctrl {**all** | *group-type-index* {**unicast** | **multicast** | **broadcast** | **all** [**rate**]}}

Parameters

all	Clear all flood control resources for all port groups.
group-type-index	Specifies a port group/type index. Valid entries are in the form of **group#.port-type**. Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as **3.0**.
unicast	Clear unicast port resources for the specified port group.
multicast	Clear multicast port resources for the specified port group.
broadcast	Clear broadcast port resources for the specified port group.
all	Clear all flood control port resources for the specified port group.
rate	(Optional) Clear the data rate limiter of the specified type of port resource to the default (none or disabled).

Defaults

None.

Mode

Switch command, read-write.

Example

This example clears the unicast port resource for port group 1.0 to default values.

```
C3(su)->clear cos port-resource flood-ctrl 1.0 unicast
```

set cos reference

Use this command to set the Class of Service inbound rate limiting reference configuration.

Syntax

set cos reference irl *group-type-index reference* **rate-limit** *irl-index*

Parameters

irl	Specifies that an IRL reference is being configured.
group-type-index	Specifies an inbound rate limiting port group/type index. Valid entries are in the form of **group#.port-type**. Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as **3.0**.
reference	IRL reference number associated with this entry.
rate-limit *irl-index*	Rate limiter (IRL resource index) to bind this reference to. Valid values range from 0 to 99.

Defaults

None.

Mode

Switch command, read-write.

Usage

The CoS reference table maps the user-defined IRL references found in the CoS settings table (see "set cos settings" on page 11-22) to rate limiters created in the port resource table (see "set cos port-resource irl" on page 11-27). The CoS reference table indexes can be thought of as virtual rate limiters. The table accounts for the maximum number of rate limiters supported by the device. The virtual limiters then map to the physical rate limiters. The CoS IRL Reference Table is not configured by default.

The CoS IRL reference table uses 100 indexes or virtual rate limiters, and maps each virtual limiter to a physical limiter or resource. An IRL reference table exists for each port group configured, and is indexed similarly to port resources, as port group#, port-type, reference. IRL references are not populated with limiters (resources), but can be configured by the user. The IRL reference table can be displayed using the show cos reference command.

Example

In the CoS IRL reference mapping table for port groups 1.0 and 2.0, create a reference for the IRL resource number 1 created for each group. The reference number 1 is used.

```
C3(su)->set cos reference irl 1.0 1 rate-limit 1
C3(su)->set cos reference irl 2.0 1 rate-limit 1
```

show cos reference

Use this command to show the Class of Service inbound rate limiting reference configuration.

Syntax

show cos reference [**irl** [*group-type-index*]]

Parameters

irl	(Optional) Specifies that inbound rate limiting reference information should be displayed.
group-type-index	(Optional) Specifies an inbound rate limiting port group/type index. Valid entries are in the form of **group#.port-type**. Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as **3.0**.

Defaults

If **irl** is not specified, all CoS reference information is displayed.

If a specific port group is not specified, information for all port groups is displayed.

Mode

Switch command, read-only.

Example

This example shows the Class of Service IRL references for port group 1.0. Note that not all of the 100 possible references are displayed in this output example.

```
C3(su)->show cos reference irl 1.0

Group Index Reference Type Rate Limiter
----------- --------- ---- ------------
1.0         0         irl  none
1.0         1         irl  1
1.0         2         irl  none
1.0         3         irl  none
...
1.0         97        irl  none
1.0         98        irl  none
1.0         99        irl  none
```

clear cos reference

Use this command to clear the Class of Service inbound rate limiting reference configuration.

Syntax

clear cos reference irl {**all** | *group-type-index reference*}

Parameters

irl	Specifies that IRL references are being cleared.
all	Clear all groups indexes and references.

group-type-index	Specifies an inbound rate limiting port group/type index. Valid entries are in the form of **group#.port-type**. Valid values for group# can range from 0 to 7. Valid values for port-type can range from 0 to 1, although only port type 0 is currently supported. For example, port group 3 would be specified as **3.0**.
reference	Clear a specific reference for the specified port group.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the CoS inbound rate limiting reference configuration for all groups:

```
C3(su)->clear cos reference irl all
```

show cos unit

Use this command to show possible CoS unit entries.

Syntax

show cos unit [**irl** [**port-type** *index*] [**kbps**]] [**flood-ctrl** [**port-type** *index*] [**pps**]]

Parameters

irl	(Optional) Display only IRL unit information.
port-type *index*	(Optional) Display information about the specified port type. (Only port-type index 0 is supported.)
kbps	(Optional) Display kbps information.
flood-ctrl	(Optional) Display only flood control unit information.
pps	(Optional) Display pps information.

Defaults

If no parameters are entered, all Cos unit information is displayed.

Mode

Switch command, read-only.

Examples

This example shows possible unit entries for inbound rate limiting:

```
C3(su)->show cos unit irl

Type:                           Unit:
irl = inbound rate limiting     Kbps  = Kilobits per second
```

```
Port Type  Type  Unit  Maximum Rate  Minimum Rate  Granularity
---------  ----  ----  ------------  ------------  -----------
0          irl   Kbps  1000000       64            1
```

This examples shows flood control unit information.

```
C3(su)->show cos unit flood-ctrl

Type:                                  Unit:
flood-ctrl = flood control type        pps  = packets per second

Port Type       Type         Unit  Maximum Rate  Minimum Rate  Granularity
-----------     -----------  ----  ------------  ------------  -----------
0               flood-ctrl   pps   148810        0             1
```

clear cos all-entries

Use this command to clear all Class of Service entries except entries 0-7.

Syntax

clear cos all-entries

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the CoS configuration for all entries except entries 0-7:

```
C3(su)->clear cos all-entries
```

show cos port-type

Use this command to display Class of Service port type configurations.

Syntax

show cos port-type [**irl** [*port-type*]] [**flood-ctrl** [*port-type*]]

Parameters

irl	(Optional) Displays inbound rate limiting information.
flood-ctrl	(Optional) Displays flood control information.
port-type	(Optional) Displays information for a specific port type. (Only port type 0 is supported.)

Defaults

If no parameters are specified, inbound rate limiting and flood control information for all port types is displayed.

Mode

Switch command, read-only.

Usage

The C3 implementation provides one default port type (0) for designating available inbound rate limiting or flood control resources. Port type 0 includes all ports.

The port type 0 IRL description is “C3 100 IRL,” which indicates that this port type provides a maximum of 100 inbound rate limiting resources per port group. The port type 0 flood control description is “C3 3 flood-ctrl” which indicates that this port type provides a maximum of 3 flood control resources per port group.

Examples

This example shows inbound rate limiting information for port type 0.

```
C3(su)->show cos port-type irl 0

Number of resources:             Supported rate types:
irl = inbound rate limiter(s)    Kbps  = kilobits per second

       Port type     Number of  Supported  Eligible          Unselected
Index  description   limiters   rate type  ports             ports
-----  ------------  ---------  ---------  ----------------  ----------------
0      C3 100 IRL    100        kbps       ge.1.1-48         ge.1.1-4
```

This example shows flood control information for port type 0.

```
C3(su)->show cos port-type flood-ctrl 0

Number of resources:               Supported rate types:
flood-ctrl = flood control type    Pps  = Packets per second

       Port type      Number of  Supported  Eligible          Unselected
Index  description    limiters   rate type  ports             ports
-----  ------------   ---------  ---------  ----------------  ------------
0      C3 3 flood-ctrl   3        pps       ge.1.1-24         ge.1.1-24
```

12

Port Priority Configuration

This chapter describes the Port Priority set of commands and how to use them. Refer to the "Configuring QoS" Feature Guide for detailed information about configuring quality of service on the SecureStack C3. The Enterasys Networks firmware Feature Guides are available at:

http://www.enterasys.com/support/manuals

Port Priority Configuration Summary

The SecureStack C3 device supports Class of Service (CoS), which allows you to assign mission-critical data to higher priority through the device by delaying less critical traffic during periods of congestion. The higher priority traffic through the device is serviced first before lower priority traffic. The Class of Service capability of the device is implemented by a priority queueing mechanism. Class of Service is based on the IEEE 802.1D (802.1p) standard specification, and allows you to define eight priorities (0 through 7) and assign them to transmit queues for each port.

A priority 0 through 7 can be set on each port, with 0 being the lowest priority. A port receiving a frame without priority information in its tag header is assigned a priority according to the default priority setting on the port. For example, if the priority of a port is set to 4, the frames received through that port without a priority indicated in their tag header are classified as a priority 4 and transmitted according to that priority.

Note: When CoS override is enabled using the **set policy profile** command as described in "set policy profile" on page 11-4, CoS-based classification rules will take precedence over priority settings configured with the **set port priority** command described in this section.

Configuring Port Priority

Purpose

To view or configure port priority characteristics as follows:

- Display or change the port default Class-of Service (CoS) transmit priority (0 through 7) of each port for frames that are received (ingress) without priority information in their tag header.
- Display the current traffic class mapping-to-priority of each port.
- Set each port to transmit frames according to 802.1D (802.1p) priority set in the frame header.

Commands

For information about...	Refer to page...
show port priority	12-4
set port priority	12-3
clear port priority	12-3

show port priority

Use this command to display the 802.1D priority for one or more ports.

Syntax

show port priority [*port-string*]

Parameters

port-string	(Optional) Displays priority information for a specific port. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, priority for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display the port priority for the ge.2.1 through 5.

```
C3(su)->show port priority ge.2.1-5
ge.2.1 is set to 0
ge.2.2 is set to 0
ge.2.3 is set to 0
ge.2.4 is set to 0
ge.2.5 is set to 0
```

set port priority

Use this command to set the 802.1D (802.1p) Class-of-Service transmit priority (0 through 7) on each port. A port receiving a frame without priority information in its tag header is assigned a priority according to the priority setting on the port. For example, if the priority of a port is set to 5, the frames received through that port without a priority indicated in their tag header are classified as a priority 5.

A frame with priority information in its tag header is transmitted according to that priority.

Syntax

`set port priority` *`port-string priority`*

Parameters

port-string	Specifies the port for which to set priority. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
priority	Specifies a value of **0 to 7** to set the CoS priority for the port entered in the *port-string*. Priority value of 0 is the lowest priority.

Defaults

None.

Mode

Switch command, read-write.

Usage

The **set port priority** command will not change the 802.1p priority tag on tagged traffic with a default priority tag. The command only has an effect on how untagged traffic will be prioritized as it passes internally through the device.

Example

This example shows how to set a default priority of 6 on ge.1.3. Frames received by this port without priority information in their frame header are set to the default setting of 6:

```
C3(su)->set port priority ge.1.3 6
```

clear port priority

Use this command to reset the current CoS port priority setting to 0. This will cause all frames received without a priority value in its header to be set to priority 0.

Syntax

`clear port priority` *`port-string`*

Parameters

port-string	Specifies the port for which to clear priority. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset ge.1.11 to the default priority:

```
C3(rw)->clear port priority ge.1.11
```

Configuring Priority to Transmit Queue Mapping

Purpose

To perform the following:

- View the current priority to transmit queue mapping of each physical port.
- Configure each port to either transmit frames according to the port priority, set using the **set port priority** command described in "set port priority" on page 12-3, or according to a priority based on a percentage of port transmission capacity, assigned to transmit queues using the **set port txq** command described in "set port txq" on page 12-8.
- Clear current port priority queue settings for one or more ports.

Commands

show port priority-queue

Use this command to display the port priority levels (0 through 7, with 0 as the lowest level) associated with the current transmit queues (0 being the lowest priority) for each selected port. A frame with a certain port priority is transmitted according to the settings entered using the **set port priority-queue** command described in "set port priority-queue" on page 12-5.

Syntax

show port priority-queue [*port-string*]

Parameters

port-string	(Optional) Displays the mapping of priorities to transmit queues for one or more ports.

Defaults

If *port-string* is not specified, priority queue information for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display priority queue information for ge.1.1. In this case, frames with a priority of 0 are associated with transmit queue 1; frames with 1 or 2 priority, are associated with transmit queue 0; and so forth:

```
C3(su)->show port priority-queue ge.1.1
 Port     P0 P1 P2 P3 P4 P5 P6 P7
--------- -- -- -- -- -- -- -- --
ge.1.1    1  0  0  2  3  4  5  5
```

set port priority-queue

Use this command to map 802.1D (802.1p) priorities to transmit queues.

Syntax

set port priority-queue *port-string priority queue*

Parameters

port-string	Specifies the port(s) for which to set priority-to-queue mappings. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
priority	Specifies a value of **0** through **7** (0 is the lowest level) that determines what priority frames will be transmitted on the transmit queue entered in this command.
queue	Specifies a value of **0** through **5** (0 is the lowest level) that determines the queue on which to transmit the frames with the port priority entered in this command. **Note:** Although there are 8 queues, only queues 0 through 5 may be configured. Queues 6 and 7 are reserved for management traffic.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command enables you to change the transmit queue (0 to 5, with 0 being the lowest priority queue) for each port priority of the selected port. You can apply the new settings to one or more ports.

Example

This example shows how to set priority 5 frames received on ge.2.12 to transmit on queue 0.

```
C3(su)->set port priority-queue ge.2.12 5 0
```

clear port priority-queue

Use this command to reset port priority queue settings back to defaults for one or more ports.

Syntax

clear port priority-queue *port-string*

Parameters

port-string	Specifies the port for which to clear priority-to-queue mappings. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the priority queue settings on ge.2.12:

```
C3(su)->clear port priority-queue ge.2.12
```

Configuring Quality of Service (QoS)

Refer to the "Configuring QoS" Feature Guide for detailed information about configuring quality of service on the SecureStack C3. The Enterasys Networks firmware Feature Guides are available at:

http://www.enterasys.com/support/manuals

Purpose

Eight transmit queues are implemented in the switch hardware for each port. The commands in this section allow you to set the priority mode and weight for each of the available queues (0 through 7) for each physical port on the switch. Priority mode and weight cannot be configured on LAGs, only on the physical ports that make up the LAG.

Commands

show port txq

Use this command to display QoS transmit queue information for one or more physical ports.

Syntax

show port txq [*port-string*]

Parameters

port-string	(Optional) Specifies port(s) for which to display QoS settings. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1. Only physical ports will be displayed. LAG ports have no transmit queue information.

Defaults

If the *port-string* is not specified, the QoS setting of all physical ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display the current algorithm and transmit queue weights configured on port ge.1.10:

```
C3(su)->show port txq ge.1.10
Port    Alg  Q0  Q1  Q2  Q3  Q4  Q5  Q6  Q7
-----   --- --- --- --- --- --- --- --- ---

ge.1.10 WRR 10   10  15  20  25  20  0   0
```

set port txq

Use this command to set QoS transmit queue arbitration values for physical ports.

Syntax

set port txq *port-string value0 value1 value2 value3 value4 value5 value6 value7*

Parameters

port-string	Specifies port(s) on which to set queue arbitration values. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1. Only physical ports can be configured with this command. LAG ports cannot be configured.
value0 - value7	Specifies percentage to allocate to a specific transmit queue. The values must total 100 percent.

Defaults

None.

Mode

Switch command, read-write.

Usage

Queues can be set for strict priority (SP) or weighted round-robin (WRR). If set for WRR mode, weights may be assigned to those queues with this command. Weights are specified in the range of 0 to 100 percent. Weights specified for queues 0 through 7 on any port must total 100 percent.

Examples

This example shows how to change the arbitration values for the eight transmit queues belonging to ge.1.1:

```
C3(su)->set port txq ge.1.1 10 10 10 10 10 10 10 30
```

This example shows how to change the algorithm to strict priority for the eight transmit queues belonging to ge.1.1:

```
C3(su)->set port txq ge.1.1 0 0 0 0 0 O O 100
C3(su)->show port txq ge.1.1
Port    Alg  Q0  Q1  Q2  Q3  Q4  Q5  Q6  Q7
-----   --- --- --- --- --- --- --- --- ---

ge.1.1  STR SP  SP  SP  SP  SP  SP  SP  SP
```

clear port txq

Use this command to clear port transmit queue values back to their default values.

Syntax

clear port txq *port-string*

Parameters

port-string	Clears transmit queue values on specific port(s) back to their default values. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1. Only physical ports can be configured with this command. LAG ports cannot be configured.

Defaults

By default, transmit queues are defined as follows:

Queue	Mode	Weight	Queue	Mode	Weight
0	WRR	1	4	WRR	5
1	WRR	2	5	WRR	6
2	WRR	3	6	WRR	7
3	WRR	4	7	WRR	8

Mode

Switch command, read-write.

Example

This example shows how to clear transmit queue values on ge.1.1:

```
C3(su)->clear port txq ge.1.1
```

13

IGMP Configuration

This chapter describes the IGMP Configuration set of commands and how to use them.

IGMP Overview

About IP Multicast Group Management

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately neighboring multicast device. The protocol's mechanisms allow a host to inform its local device that it wants to receive transmissions addressed to a specific multicast group.

A multicast-enabled device can periodically ask its hosts if they want to receive multicast traffic. If there is more than one device on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the responsibility of querying the LAN for group members.

Based on the group membership information learned from IGMP, a device can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer-3, multicast devices use this information, along with a multicast routing protocol, to support IP multicasting across an IP network.

IGMP provides the final step in an IP multicast packet delivery service, since it is only concerned with forwarding multicast traffic from the local device to group members on a directly attached subnetwork or LAN segment.

This device supports IP multicast group management by passively snooping on the IGMP query and IGMP report packets transferred between IP multicast devices and IP multicast host groups to learn IP multicast group members.

The purpose of IP multicast group management is to optimize a switched network's performance so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast devices instead of flooding to all ports in the subnet (VLAN).

In addition to passively monitoring IGMP query and report messages, the SecureStack C3 can also actively send L3 IGMP query messages to learn locations of multicast devices and member hosts in multicast groups within each VLAN.

However, note that IGMP neither alters nor routes any IP multicast packets. Since IGMP is not concerned with the delivery of IP multicast packets across subnetworks, multicast routing is needed if IP multicast packets have to be routed across different subnetworks.

About Multicasting

Multicasting is used to support real-time applications such as video conferences or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed to the hosts that subscribed to this service.

The SecureStack C3 switch device uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The device looks up the IP Multicast Group used for this service and adds it to the egress list of the Level 3 interface. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Note: An Enterasys Networks Feature Guide document containing an in-depth discussion of multicast configuration is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

Configuring IGMP at Layer 2

Purpose

To configure IGMP snooping from the switch CLI.

Commands

For information about...	Refer to page...
show igmpsnooping	13-3
set igmpsnooping adminmode	13-3
set igmpsnooping interfacemode	13-4
set igmpsnooping groupmembershipinterval	13-4
set igmpsnooping maxresponse	13-5
set igmpsnooping mcrtrexpiretime	13-6
set igmpsnooping add-static	13-6
set igmpsnooping remove-static	13-7
show igmpsnooping static	13-8
show igmpsnooping mfdb	13-8
clear igmpsnooping	13-9

show igmpsnooping

Use this command to display IGMP snooping information.

Syntax

```
show igmpsnooping
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Usage

Configured information is displayed whether or not IGMP snooping is enabled. Status information is displayed only when the function is enabled. For information on enabling IGMP on the system, refer to "set igmpsnooping adminmode" on page 13-3. For information on enabling IGMP on one or more ports, refer to "set igmpsnooping interfacemode" on page 13-4.

Example

This example shows how to display IGMP snooping information:

```
C3(su)->show igmpsnooping
Admin Mode..................................... Enable
Group Membership Interval...................... 260
Max Response Time.............................. 100
Multicast Router Present Expiration Time....... 0
Interfaces Enabled for IGMP Snooping........... ge.1.1,ge.1.2,ge.1.3
Multicast Control Frame Count.................. 0
Data Frames Forwarded by the CPU............... 0
```

set igmpsnooping adminmode

Use this command to enable or disable IGMP on the system.

Syntax

```
set igmpsnooping adminmode {enable | disable}
```

Parameters

enable | **disable**	Enables or disables IGMP snooping on the system.

Defaults

None.

Mode

Switch command, read-write.

Usage

In order for IGMP snooping to be enabled on one or all ports, it must be globally enabled on the device with this command, and then enabled on a port(s) using the **set igmpsnooping interface mode** command as described in "set igmpsnooping interfacemode" on page 13-4.

Note: IGMP snooping cannot be controlled via WebView.

Example

This example shows how to enable IGMP on the system:

```
C3(su)->set igmpsnooping adminmode enable
```

set igmpsnooping interfacemode

Use this command to enable or disable IGMP on one or all ports.

Syntax

set igmpsnooping interfacemode *port-string* **{enable | disable}**

Parameters

port-string	Specifies one or more ports on which to enable or disable IGMP.
enable | **disable**	Enables or disables IGMP.

Defaults

None.

Mode

Switch command, read-write.

Usage

In order for IGMP snooping to be enabled on one or all ports, it must be globally enabled on the device using the **set igmpsnooping adminmode** command as described in "set igmpsnooping adminmode" on page 13-3, and then enabled on a port(s) using this command.

Example

This example shows how to enable IGMP on port ge.1.10:

```
C3(su)->set igmpsnooping interfacemode ge.1.10 enable
```

set igmpsnooping groupmembershipinterval

Use this command to configure the IGMP group membership interval time for the system.

Syntax

set igmpsnooping groupmembershipinterval *time*

Parameters

time	Specifies the IGMP group membership interval. Valid values are **2 - 3600** seconds. This value works together with the **set igmpsnooping maxresponsetime** command to remove ports from an IGMP group and must be greater than the max response time value.

Defaults

None.

Mode

Switch command, read-write.

Usage

The IGMP group membership interval time sets the frequency of host-query frame transmissions and must be greater than the IGMP maximum response time as described in "set igmpsnooping maxresponse" on page 13-5.

Example

This example shows how to set the IGMP group membership interval to 250 seconds:

```
C3(su)->set igmpsnooping groupmembershipinterval 250
```

set igmpsnooping maxresponse

Use this command to configure the IGMP query maximum response time for the system.

Syntax

`set igmpsnooping maxresponse` *`time`*

Parameters

time	Specifies the IGMP maximum query response time. Valid values are **100 - 255** seconds. The default value is 100 seconds. This value works together with the **set igmpsnooping groupmembershipinterval** command to remove ports from an IGMP group and must be lesser than the group membership interval value.

Defaults

None.

Mode

Switch command, read-write.

Usage

This value must be less than the IGMP maximum response time described in "set igmpsnooping groupmembershipinterval" on page 13-4.

Example

This example shows how to set the IGMP maximum response time to 100 seconds:

```
C3(su)->set igmpsnooping maxresponse 100
```

set igmpsnooping mcrtrexpiretime

Use this command to configure the IGMP multicast router expiration time for the system.

Syntax

set igmpsnooping mcrtrexpire *time*

Parameters

time	Specifies the IGMP multicast router expiration time. Valid values are **0 - 3600** seconds. A value of 0 will configure the system with an infinite expiration time. The default value is 0.

Defaults

None.

Mode

Switch command, read-write.

Usage

This timer is for expiring the switch from the multicast database. If the timer expires, and the only address left is the multicast switch, then the entry will be removed.

Example

This example shows how to set the IGMP multicast router expiration time to infinity:

```
C3(su)->set igmpsnooping mcrtrexpiretime 0
```

set igmpsnooping add-static

This command creates a new static IGMP entry or adds one or more new ports to an existing entry.

Syntax

set igmpsnooping add-static *group vlan-list* [**modify**] [*port-string*]

Parameters

group	Specifies the multicast group IP address for the entry.
vlan-list	Specifies the VLANs on which to configure the entry.
modify	(Optional) Adds the specified port or ports to an existing entry.
port-string	(Optional) Specifies the port or ports to add to the entry.

Defaults

If no ports are specified, all ports are added to the entry.

If **modify** is not specified, a new entry is created.

Mode

Switch command, read-write.

Usage

Use this command to create and configure static Layer 2 IGMP entries. Currently, up to 100 static groups can be configured. A total of 256 dynamic and static IGMP groups are supported.

Example

This example creates an IGMP entry for the multicast group with IP address of 233.11.22.33 configured on VLAN 20 configured with the port ge.1.1.

```
C3(su)->set igmpsnooping add-static 233.11.22.33 20 ge.1.1
```

set igmpsnooping remove-static

This command deletes a static IGMP entry or removes one or more new ports from an existing entry.

Syntax

set igmpsnooping remove-static *group vlan-list* [**modify**] [*port-string*]

Parameters

group	Specifies the multicast group IP address of the entry.
vlan-list	Specifies the VLANs on which the entry is configured.
modify	(Optional) Removes the specified port or ports from an existing entry.
port-string	(Optional) Specifies the port or ports to remove from the entry.

Defaults

If no ports are specified, all ports are removed from the entry.

Mode

Switch command, read-write.

Example

This example removes port ge.1.1 from the entry for the multicast group with IP address of 233.11.22.33 configured on VLAN 20.

```
C3(su)->set igmpsnooping remove-static 233.11.22.33 20 ge.1.1
```

show igmpsnooping static

This command displays static IGMP ports for one or more VLANs or IGMP groups.

Syntax

show igmpsnooping static *vlan-list* [**group** group]

Parameters

vlan-list	Specifies the VLAN for which to display static IGMP ports.
group *group*	(Optional) Specifies the IGMP group for which to display static IGMP ports.

Defaults

If no group is specified, information for all groups is displayed.

Mode

Switch command, read-only.

Example

This example displays the static IGMP ports for VLAN 20.

```
C3(su)->show igmpsnooping static 20
--------------------------------------------------------------------------------
Vlan Id      = 20   Static Multicast Group Address = 233.11.22.33     Type = IGMP
IGMP Port List = ge.1.1
```

show igmpsnooping mfdb

Use this command to display multicast forwarding database (MFDB) information.

Syntax

show igmpsnooping mfdb [**stats**]

Parameters

stats	(Optional) Displays MFDB statistics.

Defaults

If **stats** is not specified, all MFDB table entries will be displayed.

Mode

Switch command, read-only.

Examples

This example shows how to display multicast forwarding database entries:

```
C3(su)->show igmpsnooping mfdb
MAC Address         Type      Description             Interfaces
------------------  -------  ----------------  ------------------------
00:14:01:00:5E:02:CD:B0  Dynamic  Network Assist    Fwd: ge.1.1,ge.3.1,ge.4.1
00:32:01:00:5E:37:96:D0  Dynamic  Network Assist    Fwd: ge.4.7
00:32:01:00:5E:7F:FF:FA  Dynamic  Network Assist    Fwd: ge.4.7
```

This example shows how to display multicast forwarding database statistics:

```
C3(su)->show igmpsnooping mfdb stats
Max MFDB Table Entries..... 256
Most MFDB Entries Since Last Reset..... 1
Current Entries..... 0
```

clear igmpsnooping

Use this command to clear all IGMP snooping entries.

Syntax

`clear igmpsnooping`

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear all IGMP snooping entries:

```
C3(su)->clear igmpsnooping
Are you sure you want to clear all IGMP snooping entries? (y/n) y

IGMP Snooping Entries Cleared.
```

Configuring IGMP on Routing Interfaces

Router: The commands covered in this section can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to “Enabling Router Configuration Modes” on page 18-2.

Purpose

To configure IGMP on routing interfaces.

Commands

ip igmp

Use this command to enable the L3 IGMP Querier functionality on the switch. The **no** form of this command disables IGMP Querier functionality.

Syntax

```
ip igmp
no ip igmp
```

Parameters

None.

Defaults

None.

Mode

Global configuration: C3**(su)->router(Config)#**

Usage

Enabling IGMP on a routing interface requires both the ip igmp command (page 13-10), which enables it on the router, and the ip igmp enable command (page 13-11), which enables it on an interface. Once these commands are executed, the device will start sending and processing IGMP multicast traffic. IGMP is disabled by default, both globally and on a per interface basis.

Example

This example shows how to enable IGMP on the router:

```
C3(su)->router(Config)#ip igmp
```

ip igmp enable

Use this command to enable IGMP on an interface. The **no** form of this command disables IGMP on an interface.

Syntax

```
ip igmp enable
no ip igmp enable
```

Parameters

None.

Defaults

None.

Usage

Enabling IGMP on a routing interface requires both the ip igmp command (page 13-10), which enables it on the router, and the ip igmp enable command (page 13-11), which enables it on an interface. Once these commands are executed, the device will start sending and processing IGMP multicast traffic. IGMP is disabled by default, both globally and on a per interface basis.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to enable IGMP on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip igmp enable
```

ip igmp version

Use this command to set the version of IGMP running on the router. The **no** form of this command resets IGMP to the default version of 2 (IGMPv2).

Syntax

```
ip igmp version version
no ip igmp
```

Parameters

version	Specifies the IGMP version number to run on the router. Valid values are **1**, **2**, or **3**.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the IGMP version to version 1 on VLAN 1:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip igmp version 1
```

show ip igmp interface

Use this command to display information about one or more IGMP routing interfaces.

Syntax

show ip igmp interface [vlan *vlan-id]*

Parameters

vlan *vlan-id*	(Optional) Displays information for one or more VLANs.

Defaults

If not specified, information will be displayed for all VLANs configured for IGMP routing.

Mode

Any router mode.

Example

This example shows how to display IGMP routing information for VLAN 1:

```
C3(su)->router#show ip igmp interface vlan 1
Vlan 1 is Admin UP
Vlan 1 is Oper UP
IGMP is configured via the Switch
IGMP ACL currently not supported
Multicast TTL currently defaults to 1
IGMP Version is 2
Query Interval is 125 (secs)
Query Max Response Time is 100 (1/10 of a second)
Robustness is 2
Startup Query Interval is 31 (secs)
Startup Query Count is 2
Last Member Query Interval is 10 (1/10 of a second)
Last Member Query Count is 2
```

show ip igmp groups

Use this command to display a list of IGMP streams and client connection ports.

Syntax

show ip igmp groups

Parameters

None.

Defaults

None.

Mode

Any router mode.

Example

This example shows how to display information about IGMP groups:

```
C3(su)->router#show ip igmp groups
REGISTERED MULTICAST GROUP DETAILS
Multicast                                                          Version1
IP Address      Last Reporter   Up Time Expiry Time  Host Timer
--------------- --------------- ------- ------------ ------------    ----------
228.1.1.1       12.12.12.2      27
```

ip igmp query-interval

Use this command to set the IGMP query interval on a routing interface. The **no** form of this command resets the IGMP query interval to the default value of 125 seconds.

Syntax

ip igmp query-interval *time*
no ip igmp query-interval

Parameters

time	Specifies the IGMP query interval. Valid values are from **1** to **3600** seconds. Default is 125 seconds.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the IGMP query interval to 1800 seconds on VLAN 1:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip igmp query-interval 1800
```

ip igmp query-max-response-time

Use this command to set the maximum response time interval advertised in IGMPv2 queries. The **no** form of this command resets the IGMP maximum response time to the default value of 100 (one tenth of a second).

Syntax

```
ip igmp query-max-response-time time
no ip igmp query-max-response-time
```

Parameters

time	Specifies the IGMP maximum response time interval. Valid values are from **0** to **255** tenths of a second. The default value is 100 (one tenth of a second).

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the IGMP query maximum response time interval to 200 (2 tenths of a second) on VLAN 1:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip igmp query-max-response-time 200
```

ip igmp startup-query-interval

Use this command to set the interval between general IGMP queries sent on startup. The **no** form of this command resets the IGMP startup query interval to the default value of 31 seconds.

Syntax

```
ip igmp startup-query-interval time
no ip igmp startup-query-interval
```

Parameters

time	Specifies the IGMP startup query interval. Valid values are from **1** to **300** seconds. The default value is 31 seconds.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the IGMP startup query interval to 100 seconds on VLAN 1:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip igmp startup-query-interval 100
```

ip igmp startup-query-count

Use this command to set the number of IGMP queries sent out on startup, separated by the **startup-query-interval** as described in ip igmp startup-query-interval (page 13-14). The **no** form of this command resets the IGMP startup query count to the default value of 2.

Syntax

```
ip igmp startup-query-count count
no ip igmp startup-query-count
```

Parameters

count	Specifies the number of IGMP startup queries. Valid values are from **1** to **20**. The default value is 2.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the IGMP startup query count to 10 onVLAN 1:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip igmp startup-query-count 10
```

ip igmp last-member-query-interval

Use this command to set the maximum response time being inserted into group-specific queries sent in response to leave group messages. The **no** form of this command resets the IGMP last member query interval to the default value of 1 second.

Syntax

```
ip igmp last-member-query-interval time
no ip igmp last-member-query-interval
```

Parameters

time	Specifies the IGMP last member query interval. Valid values are from **0** to **255** seconds. The default value is 1 second.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the IGMP last member query interval to 10 seconds on VLAN 1:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip igmp last-member-query-interval 10
```

ip igmp last-member-query-count

Use this command to set the number of group-specific queries sent before assuming there are no local members. The **no** form of this command resets the IGMP last member query count to the default value of 2.

Syntax

```
ip igmp last-member-query-count count
no ip igmp last-member-query-count
```

Parameters

count	Specifies the number of IGMP startup queries. Valid values are from **1** to **20**. The default value is 2.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the IGMP last member query count to 10 on VLAN 1:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip igmp last-member-query-count 10
```

ip igmp robustness

Use this command to configure the robustness tuning for expected packet loss on an IGMP routing interface. The **no** form of this command resets the IGMP robustness value to the default of 2.

Syntax

```
ip igmp robustness robustness
no ip igmp robustness
```

Parameters

robustness	Specifies the IGMP robustness value. Valid values are from **1** to **255**. The default value is 2.

Defaults

None.

Mode

Interface configuration: C3 (su)->router(Config-if(Vlan 1))#

Usage

This value determines how many times IGMP messages will be sent. A higher number will mean that end stations will be more likely to see the packet. After the robustness value is reached, IGMP will assume there is no response to queries.

Example

This example shows how to set the IGMP robustness value to 5 on VLAN 1:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip igmp robustness 5
```

14

Logging and Network Management

This chapter describes switch-related logging and network management commands and how to use them.

Note: The commands in this chapter pertain to network management of the SecureStack C3 device from the **switch CLI** only. For information on router-related network management tasks, including reviewing router ARP tables and IP traffic, refer to Chapter 19.

Configuring System Logging

Note: An Enterasys Networks Feature Guide document containing an in-depth discussion of Syslog configuration is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

Purpose

To display and configure system logging, including Syslog server settings, Syslog default settings, and the logging buffer.

Commands

show logging server

Use this command to display the Syslog configuration for a particular server.

Syntax

show logging server [*index*]

Parameters

index	(Optional) Displays Syslog information pertaining to a specific server table entry. Valid values are **1**-**8**.

Defaults

If *index* is not specified, all Syslog server information will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display Syslog server configuration information:

```
C3(ro)->show logging server

IP Address       Facility Severity        Description       Port Status
-------------------------------------------------------------------------
 1 132.140.82.111 local4 warning(5)        default         514 enabled
 2 132.140.90.84  local4 warning(5)        default         514 enabled
```

Table 14-1 provides an explanation of the command output.

Table 14-1 show logging server Output Details

Output Field	What It Displays...
IP Address	Syslog server's IP address. For details on setting this using the **set logging server** command, refer to "set logging server" on page 14-3.
Facility	Syslog facility that will be encoded in messages sent to this server. Valid values are: **local0** to **local7**.
Severity	Severity level at which the server is logging messages.
Description	Text string description of this facility/server.
Port	UDP port the client uses to send to the server.
Status	Whether or not this Syslog configuration is currently enabled or disabled.

set logging server

Use this command to configure a Syslog server.

Syntax

set logging server *index* [**ip-addr** *ip-addr*] [**facility** *facility*] [**severity** *severity*] [**descr** *descr*] [**port** *port*] [**state** {**enable** | **disable**}]

Parameters

index	Specifies the server table index number for this server. Valid values are **1** - **8**.
ip-addr *ip-addr*	(Optional) Specifies the Syslog message server's IP address.
facility *facility*	(Optional) Specifies the server's facility name. Valid values are: **local0** to **local7**.
severity *severity*	(Optional) Specifies the severity level at which the server will log messages. Valid values and corresponding levels are: **1** — emergencies (system is unusable) **2** — alerts (immediate action required) **3** — critical conditions **4** — error conditions **5** — warning conditions **6** — notifications (significant conditions) **7** — informational messages **8** — debugging messages
descr *descr*	(Optional) Specifies a textual string description of this facility/server.
port *port*	(Optional) Specifies the default UDP port the client uses to send to the server.
state enable | **disable**	(Optional) Enables or disables this facility/server configuration.

Defaults

If **ip-addr** is not specified, an entry in the Syslog server table will be created with the specified *index* number and a message will display indicating that no IP address has been assigned.

If not specified, **facility**, severity and port will be set to defaults configured with the **set logging default** command ("set logging default" on page 14-5).

If **state** is not specified, the server will not be enabled or disabled.

Mode

Switch command, read-write.

Example

This command shows how to enable a Syslog server configuration for index 1, IP address 134.141.89.113, facility local4, severity level 3 on port 514:

```
C3(su)->set logging server 1 ip-addr 134.141.89.113 facility local4 severity 3
port 514 state enable
```

clear logging server

Use this command to remove a server from the Syslog server table.

Syntax

clear logging server *index*

Parameters

index	Specifies the server table index number for the server to be removed. Valid values are **1** - **8**.

Defaults

None.

Mode

Switch command, read-write.

Example

This command shows how to remove the Syslog server with index 1 from the server table:

```
C3(su)->clear logging server 1
```

show logging default

Use this command to display the Syslog server default values.

Syntax

show logging default

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This command shows how to display the Syslog server default values. For an explanation of the command output, refer back to Table 14-1 on page 14-3.

```
C3(su)->show logging default

              Facility      Severity          Port
            ----------------------------------------
Defaults:     local4       warning(5)       514
```

set logging default

Use this command to set logging default values.

Syntax

set logging default {[**facility** *facility]* [**severity** *severity*] **port** *port]*}

Parameters

facility *facility*	Specifies the default facility name. Valid values are: **local0** to **local7.**
severity *severity*	Specifies the default logging severity level. Valid values and corresponding levels are: **1** — emergencies (system is unusable) **2** — alerts (immediate action required) **3** — critical conditions **4** — error conditions **5** — warning conditions **6** — notifications (significant conditions) **7** — informational messages **8** — debugging messages
port *port*	Specifies the default UDP port the client uses to send to the server.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the Syslog default facility name to local2 and the severity level to 4 (error logging):

```
C3(su)->set logging default facility local2 severity 4
```

clear logging default

Use this command to reset logging default values.

Syntax

```
clear logging default {[facility] [severity] [port]}
```

Parameters

facility	(Optional) Resets the default facility name to **local4.**
severity	(Optional) Resets the default logging severity level to **6** (notifications of significant conditions).
port	(Optional) Resets the default UDP port the client uses to send to the server to **514**.

Defaults

At least one optional parameter must be entered.

All three optional keywords must be entered to reset all logging values to defaults.

Mode

Switch command, read-write.

Example

This example shows how to reset the Syslog default severity level to 6:

```
C3(su)->clear logging default severity
```

show logging application

Use this command to display the severity level of Syslog messages for one or all applications configured for logging on your system.

Syntax

```
show logging application [mnemonic | all]
```

Parameters

mnemonic	(Optional) Displays severity level for one application configured for logging. Mnemonics will vary depending on the number and types of applications running on your system. Sample mnemonics and their corresponding applications are listed in Table 14-3 on page 14-8. **Note:** Mnemonic values are case sensitive and must be typed as they appear in Table 14-3.
all	(Optional) Displays severity level for all applications configured for logging.

Defaults

If no parameter is specified, information for all applications will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display system logging information pertaining to the SNMP application.

```
C3(ro)->show logging application SNMP

Application   Current Severity Level
-------------------------------------------
 90     SNMP                      6

1(emergencies)  2(alerts)       3(critical)
4(errors)       5(warnings)     6(notifications)
7(information)  8(debugging)
```

Table 14-2 provides an explanation of the command output.

Table 14-2 show logging application Output Details

Output Field	What it displays...
Application	A mnemonic abbreviation of the textual description for applications being logged.
Current Severity Level	Severity level at which the server is logging messages for the listed application. This range (from 1 to 8) and its associated severity list is shown in the CLI output. For a description of these entries, which are set using the **set logging application** command, refer to "set logging application" on page 14-7.

set logging application

Use this command to set the severity level of log messages for one or all applications.

Syntax

set logging application {[*mnemonic* | **all**]} [**level** *level*]

Parameters

mnemonic	Specifies a case sensitive mnemonic abbreviation of an application to be logged. This parameter will vary depending on the number and types of applications running on your system. To display a complete list, use the **show logging application** command as described in "show logging application" on page 14-6. Sample mnemonics and their corresponding applications are listed in Table 14-3 on page 14-8. **Note:** Mnemonic values are case sensitive and must be typed as they appear in Table 14-3.
all	Sets the logging severity level for all applications.
level *level*	(Optional) Specifies the severity level at which the server will log messages for applications. Valid values and corresponding levels are: **1** — emergencies (system is unusable) **2** — alerts (immediate action required) **3** — critical conditions **4** — error conditions **5** — warning conditions **6** — notifications (significant conditions) **7** — informational messages **8** — debugging messages

Table 14-3 Mnemonic Values for Logging Applications

Mnemonic	Application
CLIWEB	Command Line Interface and Webview management
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
Driver	Hardware drivers
System	Non-application items such as general chassis management
Stacking	Stacking management (if applicable)
UPN	User Personalized Networking
Router	Router

Defaults

If **level** is not specified, none will be applied.

Mode

Switch command, read-write.

Example

This example shows how to set the severity level for SNMP to 4 so that error conditions will be logged for that application.

```
C3(rw)->set logging application SNMP level 4
```

clear logging application

Use this command to reset the logging severity level for one or all applications to the default value of 6 (notifications of significant conditions).

Syntax

clear logging application {*mnemonic* | **all**}

Parameters

mnemonic	Resets the severity level for a specific application to 6. Valid mnemonic values and their corresponding applications are listed in Table 14-3 on page 14-8.
all	Resets the severity level for all applications to 6.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the logging severity level to 6 for SNMP.

```
C3(rw)->clear logging application SNMP
```

show logging local

Use this command to display the state of message logging to the console and a persistent file.

Syntax

show logging local

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the state of message logging. In this case, logging to the console is enabled and logging to a persistent file is disabled.

```
C3(su)->show logging local
Syslog Console Logging enabled
Syslog File Logging disabled
```

set logging local

Use this command to configure log messages to the console and a persistent file.

Syntax

`set logging local console {enable | disable} file {enable | disable}`

Parameters

console enable | disable	Enables or disables logging to the console.
file enable | disable	Enables or disables logging to a persistent file.

Defaults

None.

Mode

Switch command, read-write.

Example

This command shows how to enable logging to the console and disable logging to a persistent file:

```
C3(su)->set logging local console enable file disable
```

clear logging local

Use this command to clear the console and persistent store logging for the local session.

Syntax

`clear logging local`

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear local logging:

```
C3(su)->clear logging local
```

show logging buffer

Use this command to display the last 256 messages logged. By default, critical failures and user login and logout timestamps are displayed.

Syntax

```
show logging buffer
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows a portion of the information displayed with the **show logging buffer** command:

```
C3(su)->show logging buffer
<165>Sep  4 07:43:09 10.42.71.13 CLI[5]User:rw logged in from 10.2.1.122 (telnet)
<165>Sep  4 07:43:24 10.42.71.13 CLI[5]User: debug failed login from 10.4.1.100
(telnet)
```

show logging interface

Use this command to display the interface used for the source IP address of the system logging.

Syntax

```
show logging interface
```

Parameters

None.

Defaults

None.

Mode

Switch mode, read-only.

Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the system logging.

```
C3(rw)->show logging interface
loopback 1  192.168.10.1
```

set logging interface

Use this command to specify the interface used for the source IP address of the system logging.

Syntax

set logging interface {**loopback** *loop-ID* | **vlan** *vlan-ID*}

Parameters

loopback *loop-ID*	Specifies the loopback interface to be used. The value of *loop-ID* can range from 0 to 7.
vlan *vlan-ID*	Specifies the VLAN interface to be used. The value of vlan-ID can range from 1 to 4093.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command allows you to configure the source IP address used by the system logging application when generating packets for management purposes. Any of the management interfaces, including VLAN routing interfaces, can be configured as the source IP address used in packets generated by the system logging.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the IP address of the Host interface will be used.

If a non-loopback interface is configured with this command, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the system logging source IP address.

```
C3(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
C3(rw)->router(Config-if(Vlan 100))#exit
```

```
C3(rw)->router(Config)#exit
C3(rw)->router#exit
C3(rw)->router>exit
C3(rw)->set logging interface vlan 100

C3(rw)->show logging interface
vlan 100  192.168.10.1
```

clear logging interface

Use this command to clear the interface used for the source IP address of the system logging back to the default of the Host interface.

Syntax

clear logging interface

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This command returns the interface used for the source IP address of the system logging back to the default of the Host interface.

```
C3(rw)->show logging interface
vlan 100  192.168.10.1
C3(rw)->clear logging interface
C3(rw)->
```

Monitoring Network Events and Status

Purpose

To display switch events and command history, to set the size of the history buffer, and to display and disconnect current user sessions.

Commands

history

Use this command to display the contents of the command history buffer. The command history buffer includes all the switch commands entered up to a maximum of 100, as specified in the **set history** command ("set history" on page 14-15).

Syntax

`history`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the contents of the command history buffer. It shows there are five commands in the buffer:

```
C3(su)->history
 1 hist
 2 show gvrp
 3 show vlan
 4 show igmp
 5 show ip address
```

show history

Use this command to display the size (in lines) of the history buffer.

Syntax

show history

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the size of the history buffer:

```
C3(su)->show history
 History buffer size: 20
```

set history

Use this command to set the size of the history buffer.

Syntax

set history *size* [**default**]

Parameters

size	Specifies the size of the history buffer in lines. Valid values are **1** to **100**.
default	(Optional) Makes this setting persistent for all future sessions.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the size of the command history buffer to 30 lines:

```
C3(su)->set history 30
```

ping

Use this command to send ICMP echo-request packets to another node on the network from the switch CLI.

Syntax

ping *host*

Parameters

host	Specifies the IP address of the device to which the **ping** will be sent.

Defaults

None.

Mode

Switch command, read-write.

Examples

This example shows how to ping IP address 134.141.89.29. In this case, this host is alive:

```
C3(su)->ping 134.141.89.29
134.141.89.29 is alive
```

In this example, the host at IP address is not responding:

```
C3(su)->ping 134.141.89.255
no answer from 134.141.89.255
```

show users

Use this command to display information about the active console port or Telnet session(s) logged in to the switch.

Syntax

show users

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to use the **show users** command. In this output, there are two Telnet users logged in with Read-Write access privileges from IP addresses 134.141.192.119 and 134.141.192.18:

```
C3(su)->show users
  Session  User  Location
  -------- ----- -------------------------
* telnet   rw    134.141.192.119
  telnet   rw    134.141.192.18
```

disconnect

Use this command to close an active console port or Telnet session from the switch CLI.

Syntax

disconnect {*ip-addr* | **console**}

Parameters

ip-addr	Specifies the IP address of the Telnet session to be disconnected. This address is displayed in the output shown in "show users" on page 12-15.
console	Closes an active console port.

Defaults

None.

Mode

Switch command, read-write.

Examples

This example shows how to close a Telnet session to host 134.141.192.119:

```
C3(su)->disconnect 134.141.192.119
```

This example shows how to close the current console session:

```
C3(su)->disconnect console
```

show netstat

Use this command to display network layer statistics.

Syntax

show netstat

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

The following example shows the output of this command.

```
C3(su)->show netstat
Prot Local Address                 Foreign Address               State
---- ----------------------------  ----------------------------  -----------
TCP  127.0.0.1.2222                0.0.0.0.*                     LISTEN
TCP  0.0.0.0.80                    0.0.0.0.*                     LISTEN
TCP  0.0.0.0.23                    0.0.0.0.*                     LISTEN
TCP  10.1.56.17.23                 134.141.99.104.47718          ESTABLISHED
UDP  0.0.0.0.17185                 0.0.0.0.*
UDP  127.0.0.1.49152               127.0.0.1.17185
UDP  0.0.0.0.161                   0.0.0.0.*
UDP  0.0.0.0.*                     0.0.0.0.*
UDP  0.0.0.0.514                   0.0.0.0.*
```

The following table describes the output of this command.

Table 14-4 show netstat Output Details

Output Field	What it displays...
Prot	Type of protocol running on the connection.
Local Address	IP address of the connection's local host.
Foreign Address	IP address of the connection's foreign host.
State	Communications mode of the connection.

Managing Switch Network Addresses and Routes

Purpose

To display or delete switch ARP table entries, and to display MAC address information.

Commands

show arp

Use this command to display the switch's ARP table.

Syntax

```
show arp
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the ARP table:

```
C3(su)->show arp

LINK LEVEL ARP TABLE
IP Address       Phys Address       Flags   Interface
-------------------------------------------------------
10.20.1.1        00-00-5e-00-01-1   S       host
134.142.21.194   00-00-5e-00-01-1   S       host
134.142.191.192  00-00-5e-00-01-1   S       host
134.142.192.18   00-00-5e-00-01-1   S       host
134.142.192.119  00-00-5e-00-01-1   S       host
-------------------------------------------------------
```

Table 14-5 provides an explanation of the command output.

Table 14-5 show arp Output Details

Output Field	What It Displays...
IP Address	IP address mapped to MAC address.
Phys Address	MAC address mapped to IP address.
Flags	Route status. Possible values and their definitions include: **S** - manually configured entry (static) **P** - respond to ARP requests for this entry

set arp

Use this command to add mapping entries to the switch's ARP table.

Syntax

set arp *ip-address mac-address*

Parameters

ip-address	Specifies the IP address to map to the MAC address and add to the ARP table.
mac-address	Specifies the MAC address to map to the IP address and add to the ARP table. The MAC address can be formatted as xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to map IP address 192.168.219.232 to MAC address 00-00-0c-40-0f-bc:

```
C3(su)->set arp 192.168.219.232 00-00-0c-40-0f-bc
```

clear arp

Use this command to delete a specific entry or all entries from the switch's ARP table.

Syntax

clear arp {*ip-address* | **all**}

Parameters

ip-address | **all**	Specifies the IP address in the ARP table to be cleared, or clears all ARP entries.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to delete entry 10.1.10.10 from the ARP table:

```
C3(su)->clear arp 10.1.10.10
```

traceroute

Use this command to display a hop-by-hop path through an IP network from the device to a specific destination host. Three UDP or ICMP probes will be transmitted for each hop between the source and the traceroute destination.

Syntax

traceroute [**-w** *waittime*] [**-f** *first-ttl*] [**-m** *max-ttl*] [**-p** *port*] [**-q** *nqueries*] [**-r**] [**-d**] [**-n**] [**-v**] *host*

Parameters

-w *waittime*	(Optional) Specifies time in seconds to wait for a response to a probe.
-f *first-ttl*	(Optional) Specifies the time to live (TTL) of the first outgoing probe packet.
-m *max-ttl*	(Optional) Specifies the maximum time to live (TTL) used in outgoing probe packets.
-p *port*	(Optional) Specifies the base UDP port number used in probes.
-q *nqueries*	(Optional) Specifies the number of probe inquiries.
-r	(Optional) Bypasses the normal host routing tables.
-d	(Optional) Sets the debug socket option.
-n	(Optional) Displays hop addresses numerically. (Supported in a future release.)

-v	(Optional) Displays verbose output, including the size and destination of each response.
host	Specifies the host to which the route of an IP packet will be traced.

Defaults

If not specified, *waittime* will be set to **5** seconds.

If not specified, *first-ttl* will be set to **1** second.

If not specified, *max-ttl* will be set to **30** seconds.

If not specified, *port* will be set to **33434**.

If not specified, *nqueries* will be set to **3**.

If **-r** is not specified, normal host routing tables will be used.

If **-d** is not specified, the debug socket option will not be used.

If **-v** is not specified, summary output will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to use traceroute to display a round trip path to host 192.167.252.17. In this case, hop 1 is the SecureStack C3 switch, hop 2 is 14.1.0.45, and hop 3 is back to the host IP address. Round trip times for each of the three UDP probes are displayed next to each hop:

```
C3(su)->traceroute 192.167.252.17
traceroute to 192.167.252.17 (192.167.252.17), 30 hops max, 40 byte packets
  1  matrix.enterasys.com (192.167.201.40)  20.000 ms  20.000 ms  20.000 ms
  2  14.1.0.45 (14.1.0.45)  40.000 ms  10.000 ms  20.000 ms
  3  192.167.252.17 (192.167.252.17)  50.000 ms  0.000 ms  20.000 ms
```

show mac

Use this command to display MAC addresses in the switch's filtering database. These are addresses learned on a port through the switching process.

Syntax

show mac [**address** *mac-address*] [**fid** *fid*] [**port** *port-string*] [**type** {**other** | **learned** | **self** | **mgmt**}]

Parameters

address *mac-address*	(Optional) Displays a specific MAC address (if it is known by the device).
fid *fid*	(Optional) Displays MAC addresses for a specific filter database identifier.
port *port-string*	(Optional) Displays MAC addresses for specific port(s).
type other |**learned** | **self** | **mgmt**	(Optional) Displays information related to **other**, **learned**, **self** or **mgmt** (management) address type.

Defaults

If no parameters are specified, all MAC addresses for the device will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display MAC address information for ge.3.1:

```
C3(su)->show mac port ge.3.1

MAC Address       FID  Port          Type
----------------- ---- ------------- --------
00-09-6B-0F-13-E6 15   ge.3.1        Learned

MAC Address       VLAN Port          Type    Status  Egress Ports
----------------- ---- ------------- ------- ------- --------------------------
01-01-23-34-45-56 20   any           mcast   perm    ge.3.1
```

Table 14-6 provides an explanation of the command output.

Table 14-6 show mac Output Details

Output Field	What It Displays...
MAC Address	MAC addresses mapped to the port(s) shown.
FID	Filter database identifier.
Port	Port designation.
Type	Address type. Valid types are: • Learned • Self • Management • Other (this will include any static MAC locked addresses as described in "Configuring MAC Locking" on page 26-54). • mcast (multicast)
VLAN	The VLAN ID configured for the multicast MAC address.
Status	The status of the multicast address.
Egress Ports	The ports which have been added to the egress ports list.

show mac agetime

Use this command to display the timeout period for aging learned MAC entries.

Syntax

show mac agetime

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the MAC timeout period:

```
C3(su)->show mac agetime
Aging time: 300 seconds
```

set mac agetime

Use This command to set the timeout period for aging learned MAC entries.

Syntax

set mac agetime *time*

Parameters

time	Specifies the timeout period in seconds for aging learned MAC addresses. Valid values are 10 to 1,000,000 seconds. Default value is 300 seconds.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to set the MAC timeout period:

```
C3(su)->set mac agetime 250
```

clear mac agetime

Use this command to reset the timeout period for aging learned MAC entries to the default value of 300 seconds.

Syntax

clear mac agetime

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to reset the MAC timeout period to the default value of 300 seconds.

```
C3(su)->clear mac agetime
```

set mac algorithm

Use this command to set the MAC algorithm mode, which determines the hash mechanism used by the device when performing Layer 2 lookups on received frames.

Syntax

```
set mac algorithm {mac-crc16-lowerbits | mac-crc16-upperbits |
mac-crc32-lowerbits | mac-crc32-upperbits}
```

Parameters

mac-crc16-lowerbits	Select the MAC CRC 16 lower bits algorithm for hashing.
mac-crc16-upperbits	Select the MAC CRC 16 upper bits algorithm for hashing.
mac-crc32-lowerbits	Select the MAC CRC 32 lower bits algorithm for hashing.
mac-crc32-upperbits	Select the MAC CRC 32 upper bits algorithm for hashing.

Defaults

The default MAC algorithm is **mac-crc16-upperbits**.

Mode

Switch command, read-write.

Usage

Each algorithm is optimized for a different spread of MAC addresses. When changing this mode, the switch will display a warning message and prompt you to restart the device.

The default MAC algorithm is mac-crc16-upperbits.

Example

This example sets the hashing algorithm to mac-crc32-upperbits.

```
C3(rw)->set mac algorithm mac-crc32-upperbits
```

show mac algorithm

This command displays the currently selected MAC algorithm mode.

Syntax

```
show mac algorithm
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows the output of this command.

```
C3(su)->show mac algorithm
Mac hashing algorithm is mac-crc16-upperbits.
```

clear mac algorithm

Use this command to return the MAC hashing algorithm to the default value of **mac-crc16-upperbits.**

Syntax

clear mac algorithm

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example resets the MAC hashing algorithm to the default value.

```
C3(su)->clear mac algorithm
```

set mac multicast

Use this command to define on what ports within a VLAN a multicast address can be dynamically learned on, or on what ports a frame with the specified MAC address can be flooded. Also, use this command to append ports to or clear ports from the egress ports list.

Syntax

set mac multicast *mac-address vlan-id* [*port-string*] [{**append** | **clear**} *port-string*]

Parameters

mac-address	Specifies the multicast MAC address. The MAC address can be formatted as xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.
vlan-id	Specifies the VLAN ID containing the ports.
port-string	Specifies the port or range of ports the multicast MAC address can be learned on or flooded to.
append | **clear**	Appends or clears the port or range of ports from the egress port list.

Defaults

If no *port-string* is defined, the command will apply to all ports.

Mode

Switch command, read-write.

Example

This example configures multicast MAC address 01-01-22-33-44-55 for VLAN 24.

```
C3(su)->set mac multicast 01-01-22-33-44-55 24
```

clear mac address

Use this command to remove a multicast MAC address.

Syntax

clear mac address *mac-address* [*vlan-id*]

Parameters

mac-address	Specifies the multicast MAC address to be cleared. The MAC address can be formatted as xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.
vlan-id	(Optional) Specifies the VLAN ID from which to clear the static multicast MAC address.

Defaults

If no *vlan-id* is specified, the multicast MAC address is cleared from all VLANs.

Mode

Switch command, read-write.

Example

This example clears multicast MAC address 01-01-22-33-44-55 from VLAN 24.

```
C3(su)->clear mac multicast 01-01-22-33-44-55 24
```

show mac unreserved-flood

Use this command to display the state of multicast flood protection.

Syntax

```
show mac unreserved-flood
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example displays the status of multicast flood protection.

```
C3(su)->show mac unreserved-flood
mac unreserved flood is disabled.
```

set mac unreserved-flood

Use this command to enable or disable multicast flood protection. When enabled, this prevents policy profiles requiring a full 10 masks from being loaded.

Syntax

```
set mac unreserved-flood {disable | enable}
```

Parameters

disable | **enable**	Disables or enables multicast flood protection.

Defaults

None.

Mode

Switch command, read-write.

Usage

The following addresses will be forwarded when this function is enabled:

01:80:C2:00:00:11

01:80:C2:00:00:14

01:80:C2:00:00:15

The default state is disabled, and these addresses will not be forwarded.

Example

This example enables multicast flood protection.

```
C3(su)->set mac unreserved-flood enable
```

Configuring Simple Network Time Protocol (SNTP)

Purpose

To configure the Simple Network Time Protocol (SNTP), which synchronizes device clocks in a network.

Note: A management IP (host, routing interface, or loopback) address must be configured for SNTP to work..

Commands

For information about...	Refer to page...
show sntp	14-29
set sntp client	14-31
clear sntp client	14-31
set sntp server	14-32
clear sntp server	14-32
set sntp poll-interval	14-33
clear sntp poll-interval	14-33
set sntp poll-retry	14-34
clear sntp poll-retry	14-34
set sntp poll-timeout	14-35
clear sntp poll-timeout	14-35
set timezone	14-36
show sntp interface	14-37
set sntp interface	14-37
clear sntp interface	14-38

show sntp

Use this command to display SNTP client settings.

Syntax

`show sntp`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display SNTP client settings:

```
C3(su)->show sntp
SNTP Version: 3
Current Time: TUE SEP 09 16:13:33 2003
Timezone: 'EST', offset from UTC is -4 hours and 0 minutes
Client Mode: unicast
Broadcast Count: 0
Poll Interval: 512 seconds
Poll Retry: 1
Poll Timeout: 5 seconds
SNTP Poll Requests: 1175
Last SNTP Update: TUE SEP 09 16:05:24 2003
Last SNTP Request: TUE SEP 09 16:05:24 2003
Last SNTP Status: Success

SNTP-Server       Precedence       Status
----------------------------------------
10.2.8.6              2            Active
144.111.29.19         1            Active
```

Table 14-7 provides an explanation of the command output.

Table 14-7 show sntp Output Details

Output Field	What It Displays...
SNTP Version	SNTP version number.
Current Time	Current time on the system clock.
Timezone	Time zone name and amount it is offset from UTC (Universal Time). Set using the **set timezone** command (“set timezone” on page 14-36).
Client Mode	Whether SNTP client is operating in unicast or broadcast mode. Set using **set sntp client** command (“set sntp client” on page 14-31).
Broadcast Count	Number of SNTP broadcast frames received.
Poll Interval	Interval between SNTP unicast requests. Default of 512 seconds can be reset using the **set sntp poll-interval** command (“set sntp poll-interval” on page 14-33).
Poll Retry	Number of poll retries to a unicast SNTP server. Default of 1 can be reset using the **set sntp poll-retry** command (“set sntp poll-retry” on page 14-34).
Poll Timeout	Timeout for a response to a unicast SNTP request. Default of 5 seconds can be reset using **set sntp poll-timeout** command (“set sntp poll-timeout” on page 14-35).
SNTP Poll Requests	Total number of SNTP poll requests.

Table 14-7 show sntp Output Details (Continued)

Output Field	What It Displays...
Last SNTP Update	Date and time of most recent SNTP update.
Last SNTP Request	Date and time of most recent SNTP request.
Last SNTP Status	Whether or not broadcast reception or unicast transmission and reception was successful.
SNTP-Server	IP address(es) of SNTP server(s).
Precedence	Precedence level of SNTP server in relation to its peers. Highest precedence is 1 and lowest is 10. Default of 1 can be reset using the **set sntp server** command ("set sntp server" on page 14-32).
Status	Whether or not the SNTP server is active.

set sntp client

Use this command to set the SNTP operation mode.

Syntax

```
set sntp client {broadcast | unicast | disable}
```

Parameters

broadcast	Enables SNTP in broadcast client mode.
unicast	Enables SNTP in unicast (point-to-point) client mode. In this mode, the client must supply the IP address from which to retrieve the current time.
disable	Disables SNTP.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to enable SNTP in broadcast mode:

```
C3(su)->set sntp client broadcast
```

clear sntp client

Use this command to clear the SNTP client's operational mode.

Syntax

```
clear sntp client
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the SNTP client's operational mode:

```
C3(su)->clear sntp client
```

set sntp server

Use this command to add a server from which the SNTP client will retrieve the current time when operating in unicast mode. Up to 10 servers can be set as SNTP servers.

Syntax

set sntp server *ip-address* [*precedence*]

Parameters

ip-address	Specifies the SNTP server's IP address.
precedence	(Optional) Specifies this SNTP server's precedence in relation to its peers. Valid values are **1** (highest) to **10** (lowest).

Defaults

If *precedence* is not specified, 1 will be applied.

Mode

Switch command, read-write.

Example

This example shows how to set the server at IP address 10.21.1.100 as an SNTP server:

```
C3(su)->set sntp server 10.21.1.100
```

clear sntp server

Use this command to remove one or all servers from the SNTP server list.

Syntax

clear sntp server {*ip-address* | **all**}

Parameters

ip-address	Specifies the IP address of a server to remove from the SNTP server list.
all	Removes all servers from the SNTP server list.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to remove the server at IP address 10.21.1.100 from the SNTP server list:

```
C3(su)->clear sntp server 10.21.1.100
```

set sntp poll-interval

Use this command to set the poll interval between SNTP unicast requests.

Syntax

set sntp poll-interval *value*

Parameters

value	The poll interval is 2 to the power of *value* in seconds, where *value* can range from **6** to **10**.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the SNTP poll interval to 64 seconds:

```
C3(su)->set sntp poll-interval 6
```

clear sntp poll-interval

Use this command to clear the poll interval between unicast SNTP requests.

Syntax

clear sntp poll-interval

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the SNTP poll interval:

```
C3(su)->clear sntp poll-interval
```

set sntp poll-retry

Use this command to set the number of poll retries to a unicast SNTP server.

Syntax

set sntp poll-retry *retry*

Parameters

retry	Specifies the number of retries. Valid values are **0** to **10.**

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the number of SNTP poll retries to 5:

```
C3(su)->set sntp poll-retry 5
```

clear sntp poll-retry

Use this command to clear the number of poll retries to a unicast SNTP server.

Syntax

clear sntp poll-retry

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the number of SNTP poll retries:

```
C3(su)->clear sntp poll-retry
```

set sntp poll-timeout

Use this command to set the poll timeout (in seconds) for a response to a unicast SNTP request.

Syntax

set sntp poll-timeout *timeout*

Parameters

timeout	Specifies the poll timeout in seconds. Valid values are **1** to **30**.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the SNTP poll timeout to 10 seconds:

```
C3(su)->set sntp poll-timeout 10
```

clear sntp poll-timeout

Use this command to clear the SNTP poll timeout.

Syntax

clear sntp poll-timeout

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the SNTP poll timeout:

```
C3(su)->clear sntp poll-timeout
```

set timezone

Use this command to configure the current timezone as an offset from UTC.

Syntax

set timezone *name* [*hours*] [*minutes*]

Parameters

name	The name of the timezone. Typically, this name is a standard abbreviation such as EST (Eastern Standard Time) or EDT (Eastern Daylight Time).
hours	(Optional) Specifies the offset in hours from UTC. The value can range from -13 to 13. The default is 0 hours.
minutes	(Optional) Specifies additional offset in minutes from UTC. The value can range from 0 to 59. The default is 0 minutes.

Defaults

If you enter a timezone name without specifying an offset in hours and minutes, the default is an offset from UTC of 0 hours and 0 minutes.

Mode

Switch command, read-write.

Usage

Typically, this command is used to configure the local timezone offset from UTC (Univeral Time) when SNTP is used to synchronize the time used by devices on the network.

To display the current timezone setting used by SNTP, use the **show sntp** command. To clear an existing offset to zero, enter the command without specifying any hours or minutes.

Standard timezone names and offsets can be found at the following URL, among others:

http://www.timeanddate.com/library/abbreviations/timezones/

Example

The following example sets the timezone name to EST and the offset to North American Eastern Standard Time offset of -5 hours from UTC, then displays the timezone used with SNTP.

```
C3(su)->set timezone EST -5

C3(su)->show sntp
SNTP Version: 3
Current Time: WED JUL 16 11:35:52 2008
Timezone: 'EST' offset from UTC is -5 hours and 0 minutes
Client Mode: unicast
Broadcast Count: 0
Poll Interval: 6 (64 seconds)
Poll Retry: 1
Poll Timeout: 5 seconds
SNTP Poll Requests: 2681
Last SNTP Update: WED JUL 16 16:35:23 2008
Last SNTP Request: WED JUL 16 16:35:23 2008
Last SNTP Status: Success
```

```
SNTP-Server       Precedence       Status
-----------------------------------------
192.255.255.254        2            Active
```

show sntp interface

Use this command to display the interface used for the source IP address of the SNTP client.

Syntax

show sntp interface

Parameters

None.

Defaults

None.

Mode

Switch mode, read-only.

Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the SNTP client.

```
C3(rw)->show sntp interface
loopback 1  192.168.10.1
```

set sntp interface

Use this command to specify the interface used for the source IP address of the SNTP client.

Syntax

set sntp interface {**loopback** *loop-ID* | **vlan** *vlan-ID*}

Parameters

loopback *loop-ID*	Specifies the loopback interface to be used. The value of *loop-ID* can range from 0 to 7.
vlan *vlan-ID*	Specifies the VLAN interface to be used. The value of vlan-ID can range from 1 to 4093.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command allows you to configure the source IP address used by the SNTP application when generating packets for management purposes. Any of the management interfaces, including VLAN routing interfaces, can be configured as the source IP address used in packets generated by the SNTP client.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the IP address of the Host interface will be used.

If a non-loopback interface is configured with this command, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the SNTP client source IP address.

```
C3(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
C3(rw)->router(Config-if(Vlan 100))#exit
C3(rw)->router(Config)#exit
C3(rw)->router#exit
C3(rw)->router>exit
C3(rw)->set sntp interface vlan 100

C3(rw)->show sntp interface
vlan 100  192.168.10.1
```

clear sntp interface

Use this command to clear the interface used for the source IP address of the SNTP client back to the default of the Host interface.

Syntax

`clear sntp interface`

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This command returns the interface used for the source IP address of the SNTP client back to the default of the Host interface.

```
C3(rw)->show sntp interface
vlan 100  192.168.10.1
C3(rw)->clear sntp interface
C3(rw)->
```

Configuring Node Aliases

The node alias feature enables administrators to determine the MAC address and location of a given end-station (or node) using the node's Layer 3 alias information (IP address) as a key. With this method, it is possible to determine that, for instance, IP address 123.145.2.23 is located on switch 5 port 3.

The passive accumulation of a network's node/alias information is accomplished by "snooping" on the contents of network traffic as it passes through the switch fabric.

In the C3, node data is automatically accumulated into the ct-alias mib, and by default this feature is enabled. The NetSight Console Compass utility and Automated Security Manager (ASM) use the information in the node/alias MIB table.

It's important to make sure that inter-switch links are not learning node/alias information, as it would slow down searches by the NetSight Compass and ASM tools and give inaccurate results.

Purpose

To review, disable, and re-enable node (port) alias functionality on the switch.

Commands

For information about...	Refer to page...
show nodealias config	14-40
set nodealias	14-41
clear nodealias config	14-42

show nodealias config

Use this command to display node alias configuration settings on one or more ports.

Syntax

show nodealias config [*port-string*]

Parameters

port-string	(Optional) Displays node alias configuration settings for specific port(s).

Defaults

If *port-string* is not specified, node alias configurations will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display node alias configuration settings for ports ge.2.1 through 9:

```
C3(rw)->show nodealias config ge.2.1-9
Port Number        Max Entries         Used Entries        Status
```

```
-----------         -----------         ------------        ------
ge.2.1              16                  0                   Enable
ge.2.2              47                  0                   Enable
ge.2.3              47                  2                   Enable
ge.2.4              47                  0                   Enable
ge.2.5              47                  0                   Enable
ge.2.6              47                  2                   Enable
ge.2.7              47                  0                   Enable
ge.2.8              47                  0                   Enable
ge.2.9              4000                1                   Enable
```

Table 14-8 provides an explanation of the command output.

Table 14-8 show nodealias config Output Details

Output Field	What It Displays...
Port Number	Port designation.
Max Entries	Maximum number of alias entries configured for this port.
Used Entries	Number of alias entries (out of the maximum amount configured) already used by this port.
Status	Whether or not a node alias agent is enabled (default) or disabled on this port.

set nodealias

Use this command to enable or disable a node alias agent on one or more ports, or set the maximum number of alias entries stored per port.

Syntax

set nodealias {**enable** | **disable** | **maxentries** *maxentries*} *port-string*

Parameters

enable | **disable**	Enables or disables a node alias agent.
maxentries *maxentries*	Set the maximum number of alias entries stored per port. Valid range is 0 to 4096. The default value is 32.
port-string	Specifies the port(s) on which to enable/disable node alias agent or set a maximum number of stored entries.

Defaults

None.

Mode

Switch command, read-write.

Usage

Upon packet reception, node aliases are dynamically assigned to ports enabled with an alias agent, which is the default setting on SecureStack C3 devices. Node aliases cannot be statically created, but can be deleted using the command “clear nodealias config” (page 14-42).

It's important to make sure that inter-switch links are not learning node/alias information, as it would slow down searches by the NetSight Compass and ASM tools and give inaccurate results.

Example

This example shows how to disable the node alias agent on ge.1.3:

```
C3(su)->set nodealias disable ge.1.3
```

clear nodealias config

Use this command to reset node alias state to enabled and clear the maximum entries value.

Syntax

clear nodealias config *port-string*

Parameters

port-string	Specifies the port(s) on which to reset the node alias configuration.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the node alias configuration on ge.1.3:

```
C3(su)->clear nodealias config ge.1.3
```

15

RMON Configuration

This chapter describes the commands used to configure RMON on a SecureStack C3 switch.

RMON Monitoring Group Functions

RMON (Remote Network Monitoring) provides comprehensive network fault diagnosis, planning, and performance tuning information and allows for interoperability between SNMP management stations and monitoring agents. RMON extends the SNMP MIB capability by defining additional MIBs that generate a much richer set of data about network usage. These MIB "groups" each gather specific sets of data to meet common network monitoring requirements.

Table 15-1 lists the RMON monitoring groups supported on SecureStack C3 devices, each group's function and the elements it monitors, and the associated configuration commands needed.

Table 15-1 RMON Monitoring Group Functions and Commands

RMON Group	What It Does...	What It Monitors...	CLI Command(s)
Statistics	Records statistics measured by the RMON probe for each monitored interface on the device.	Packets dropped, packets sent, bytes sent (octets), broadcast and multicast packets, CRC errors, oversized and undersized packets, fragments, jabbers, and counters for packets.	"show rmon stats" on page 15-4 "set rmon stats" on page 15-4 "clear rmon stats" on page 15-5

Table 15-1 RMON Monitoring Group Functions and Commands (Continued)

RMON Group	What It Does...	What It Monitors...	CLI Command(s)
History	Records periodic statistical samples from a network.	Sample period, number of samples and item(s) sampled.	"show rmon history" on page 15-6 "set rmon history" on page 15-7 "clear rmon history" on page 15-7
Alarm	Periodically gathers statistical samples from variables in the probe and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.	Alarm type, interval, starting threshold, stop threshold.	"show rmon alarm" on page 15-9 "set rmon alarm properties" on page 15-10 "set rmon alarm status" on page 15-11 "clear rmon alarm" on page 15-12
Event	Controls the generation and notification of events from the device.	Event type, description, last time event was sent.	"show rmon event" on page 15-13 "set rmon event properties" on page 15-14 "set rmon event status" on page 15-15 "clear rmon event" on page 15-15
Filter	Allows packets to be matched by a filter equation. These matched packets form a data stream or "channel" that may be captured.	Packets matching the filter configuration.	"show rmon channel" on page 15-17 "set rmon channel" on page 15-18 "clear rmon channel" on page 15-19 "show rmon filter" on page 15-19 "set rmon filter" on page 15-20 "clear rmon filter" on page 15-21
Packet Capture	Allows packets to be captured upon a filter match.	Packets matching the filter configuration.	"show rmon capture" on page 15-22 "set rmon capture" on page 15-23 "clear rmon capture" on page 15-24

Design Considerations

The C3 supports RMON Packet Capture/Filter Sampling through both the CLI and MIBs, but with the following constraints:

- RMON Packet Capture/Filter Sampling and Port Mirroring cannot be enabled on the same interface concurrently.
- You can capture a total of 100 packets on an interface, no more and no less.
  - The captured frames will be as close to sequential as the hardware will allow.
  - Only one interface can be configured for capturing at a time.
  - Once 100 frames have been captured by the hardware, the application will stop without manual intervention.
- As described in the MIB, the filter is only applied after the frame is captured, thus only a subset of the frames captured will be available for display.
- There is only one Buffer Control Entry supported.
- Due to the limitations of the hardware, the Buffer Control Entry table will have limits on a few of its elements:
  - MaxOctetsRequested can only be set to the value -1 which indicates the application will capture as many packets as possible given its restrictions.
  - CaptureSliceSize can only be set to 1518.
  - The Full Action element can only be set to “lock” since the device does not support wrapping the capture buffer.
- Due to hardware limitations, the only frame error counted is oversized frames.
- The application does not support Events. Therefore, the following elements of the Channel Entry Table are not supported: TurnOnEventIndex, TurnOffEventIndex, EventIndex, and EventStatus.
- There is only one Channel Entry available at a time.
  - There are only three Filter Entries available, and a user can associate all three Filter Entries with the Channel Entry.
- Configured channel, filter, and buffer information will be saved across resets, but not frames within the capture buffer.

Statistics Group Commands

Purpose

To display, configure, and clear RMON statistics.

Note: Due to hardware limitations, the only frame error counted is oversized frames.

Commands

For information about...	Refer to page...
show rmon stats	15-4
set rmon stats	15-4
clear rmon stats	15-5

show rmon stats

Use this command to display RMON statistics measured for one or more ports.

Syntax

show rmon stats [*port-string*]

Parameters

port-string	(Optional) Displays RMON statistics for specific port(s).

Defaults

If *port-string* is not specified, RMON stats will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display RMON statistics for Gigabit Ethernet port 1 in switch 1.

```
C3(su)->show rmon stats ge.1.1

Port: ge.1.1
-------------------------------------
Index           = 1
Owner           = monitor
Data Source     = ifIndex.1

Drop Events     = 0       Packets             = 0
Collisions      = 0       Octets              = 0
Jabbers         = 0       0    -   64 Octets  = 0
Broadcast Pkts  = 0       65   -  127 Octets  = 0
Multicast Pkts  = 0       128  -  255 Octets  = 0
CRC Errors      = 0       256  -  511 Octets  = 0
Undersize Pkts  = 0       512  - 1023 Octets  = 0
Oversize Pkts   = 0       1024 - 1518 Octets  = 0
Fragments       = 0
```

Table 15-2 provides an explanation of the command output.

set rmon stats

Use this command to configure an RMON statistics entry.

Syntax

set rmon stats *index port-string* [*owner*]

Parameters

index	Specifies an index for this statistics entry.
port-string	Specifies port(s) to which this entry will be assigned.
owner	(Optional) Assigns an owner for this entry.

Defaults

If *owner* is not specified, **monitor** will be applied.

Mode

Switch command, read-write.

Example

This example shows how to configure RMON statistics entry 2 for ge.1.20:

```
C3(rw)->set rmon stats 2 ge.1.20
```

clear rmon stats

Use this command to delete one or more RMON statistics entries.

Syntax

clear rmon stats {*index-list* | **to-defaults**}

Parameters

index-list	Specifies one or more stats entries to be deleted, causing them to disappear from any future RMON queries.
to-defaults	Resets all history entries to default values. This will cause entries to reappear in RMON queries.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to delete RMON statistics entry 2:

```
C3(rw)->clear rmon stats 2
```

History Group Commands

Purpose

To display, configure, and clear RMON history properties and statistics.

Commands

For information about...	Refer to page...
show rmon history	15-6
set rmon history	15-7
clear rmon history	15-7

show rmon history

Use this command to display RMON history properties and statistics. The RMON history group records periodic statistical samples from a network.

Syntax

show rmon history [*port-string*]

Parameters

port-string	(Optional) Displays RMON history entries for specific port(s).

Defaults

If *port-string* is not specified, information about all RMON history entries will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display RMON history entries for Gigabit Ethernet port 1 in switch 1. A control entry displays first, followed by actual entries corresponding to the control entry. In this case, the default settings for entry owner, sampling interval, and maximum number of entries. (buckets) have not been changed from their default values. For a description of the types of statistics shown, refer to Table 15-2.

```
C3(su)->show rmon history ge.1.1

Port: ge.1.1
-------------------------------------
Index 1
Owner             = monitor
Status            = valid
Data Source       = ifIndex.1
Interval          = 30
Buckets Requested = 50
Buckets Granted   = 10
```

```
Sample  2779         Interval Start: 1 days 0 hours 2 minutes 22 seconds
Drop Events       = 0       Undersize Pkts    = 0
Octets            = 0       Oversize Pkts     = 0
Packets           = 0       Fragments         = 0
Broadcast Pkts    = 0       Jabbers           = 0
Multicast Pkts    = 0       Collisions        = 0
CRC Align Errors  = 0       Utilization(%)    = 0
```

set rmon history

Use this command to configure an RMON history entry.

Syntax

set rmon history *index* [*port-string*] [**buckets** *buckets*] [**interval** *interval*] [**owner** *owner*]

Parameters

index-list	Specifies an index number for this entry.
port-string	(Optional) Assigns this entry to a specific port.
buckets *buckets*	(Optional) Specifies the maximum number of entries to maintain.
interval *interval*	(Optional) Specifies the sampling interval in seconds.
owner *owner*	(Optional) Specifies an owner for this entry.

Defaults

If *buckets* is not specified, the maximum number of entries maintained will be 50.

If not specified, *interval* will be set to 30 seconds.

If *owner* is not specified, **monitor** will be applied.

Mode

Switch command, read-write.

Example

This example shows how configure RMON history entry 1 on port ge.2.1 to sample every 20 seconds:

```
C3(rw)->set rmon history 1 ge.2.1 interval 20
```

clear rmon history

Use this command to delete one or more RMON history entries or reset one or more entries to default values. For specific values, refer to “set rmon history” on page 15-7.

Syntax

clear rmon history {*index-list* | **to-defaults**}

Parameters

index-list	Specifies one or more history entries to be deleted, causing them to disappear from any future RMON queries.
to-defaults	Resets all history entries to default values. This will cause entries to reappear in RMON queries.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to delete RMON history entry 1:

```
C3(rw)->clear rmon history 1
```

Alarm Group Commands

Purpose

To display, configure, and clear RMON alarm entries and properties.

Commands

show rmon alarm

Use this command to display RMON alarm entries. The RMON alarm group periodically takes statistical samples from RMON variables and compares them with previously configured thresholds. If the monitored variable crosses a threshold an RMON event is generated.

Syntax

show rmon alarm [*index*]

Parameters

index	(Optional) Displays RMON alarm entries for a specific entry index ID.

Defaults

If *index* is not specified, information about all RMON alarm entries will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display RMON alarm entry 3:

```
C3(rw)->show rmon alarm 3

Index 3
---------------------
Owner               = Manager
Status              = valid
Variable            = 1.3.6.1.4.1.5624.1.2.29.1.2.1.0
Sample Type         = delta          Startup Alarm       = rising
Interval            = 30             Value               = 0
Rising Threshold    = 1              Falling Threshold   = 0
Rising Event Index  = 2              Falling Event Index = 0
```

Table 15-2 provides an explanation of the command output.

Table 15-2 show rmon alarm Output Details

Output Field	What It Displays...
Index	Index number for this alarm entry.
Owner	Text string identifying who configured this entry.
Status	Whether this event entry is enabled (valid) or disabled.
Variable	MIB object to be monitored.
Sample Type	Whether the monitoring method is an absolute or a delta sampling.
Startup Alarm	Whether alarm generated when this entry is first enabled is rising, falling, or either.
Interval	Interval in seconds at which RMON will conduct sample monitoring.
Rising Threshold	Minimum threshold for causing a rising alarm.
Falling Threshold	Maximum threshold for causing a falling alarm.
Rising Event Index	Index number of the RMON event to be triggered when the rising threshold is crossed.
Falling Event Index	Index number of the RMON event to be triggered when the falling threshold is crossed.

set rmon alarm properties

Use this command to configure an RMON alarm entry, or to create a new alarm entry with an unused alarm index number.

Syntax

```
set rmon alarm properties index [interval interval] [object object] [type
{absolute | delta}] [startup {rising | falling | either}] [rthresh rthresh]
[fthresh fthresh] [revent revent] [fevent fevent] [owner owner]
```

Parameters

index	Specifies an index number for this entry. Maximum number or entries is 50**.** Maximum value is **65535.**
interval *interval*	(Optional) Specifies an interval (in seconds) for RMON to conduct sample monitoring.
object *object*	(Optional) Specifies a MIB object to be monitored.  **Note:** This parameter is not mandatory for executing the command, but must be specified in order to enable the alarm entry configuration.
type absolute | **delta**	(Optional) Specifies the monitoring method as: sampling the absolute value of the object, or the difference (delta) between object samples.

startup rising | **falling** | **either**	(Optional) Specifies the type of alarm generated when this event is first enabled as: • Rising - Sends alarm when an RMON event reaches a maximum threshold condition is reached, for example, more than 30 collisions per second. • Falling - Sends alarm when RMON event falls below a minimum threshold condition, for example when the network is behaving normally again. • Either - Sends alarm when either a rising or falling threshold is reached.
rthresh *rthresh*	(Optional) Specifies a minimum threshold for causing a rising alarm.
fthresh *fthresh*	Specifies a maximum threshold for causing a falling alarm.
revent *revent*	Specifies the index number of the RMON event to be triggered when the rising threshold is crossed.
fevent *fevent*	Specifies the index number of the RMON event to be triggered when the falling threshold is crossed.
owner *owner*	(Optional) Specifies the name of the entity that configured this alarm entry.

Defaults

interval - **3600** seconds

type - **absolute**

startup - **rising**

rthresh - **0**

fthresh - **0**

revent - **0**

fevent - **0**

owner - **monitor**

Mode

Switch command, read-write.

Example

This example shows how to configure a rising RMON alarm. This entry will conduct monitoring of the delta between samples every 30 seconds:

```
C3(rw)->set rmon alarm properties 3 interval 30 object
   1.3.6.1.4.1.5624.1.2.29.1.2.1.0 type delta rthresh 1 revent 2 owner Manager
```

set rmon alarm status

Use this command to enable an RMON alarm entry. An alarm is a notification that a statistical sample of a monitored variable has crossed a configured threshold.

Syntax

set rmon alarm status *index* **enable**

Parameters

index	Specifies an index number for this entry. Maximum number or entries is 50**.** Maximum value is **65535.**
enable	Enables this alarm entry.

Defaults

None.

Mode

Switch command, read-write.

Usage

An RMON alarm entry can be created using this command, configured using the **set rmon alarm properties** command ("set rmon alarm properties" on page 15-10), then enabled using this command. An RMON alarm entry can be created and configured at the same time by specifying an unused index with the **set rmon alarm properties** command.

Example

This example shows how to enable RMON alarm entry 3:

```
C3(rw)->set rmon alarm status 3 enable
```

clear rmon alarm

Use this command to delete an RMON alarm entry.

Syntax

clear rmon alarm *index*

Parameters

index	Specifies the index number of entry to be cleared.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear RMON alarm entry 1:

```
C3(rw)->clear rmon alarm 1
```

Event Group Commands

Purpose

To display and clear RMON events, and to configure RMON event properties.

Commands

show rmon event

Use this command to display RMON event entry properties.

Syntax

show rmon event [*index*]

Parameters

index	(Optional) Displays RMON properties and log entries for a specific entry index ID.

Defaults

If *index* is not specified, information about all RMON entries will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display RMON event entry 3:

```
C3(rw)->show rmon event 3

Index 3
----------------
Owner          = Manager
Status         = valid
Description    = STP Topology change
Type           = log-and-trap
Community      = public
Last Time Sent = 0 days 0 hours 0 minutes 37 seconds
```

Table 15-3 provides an explanation of the command output.

Table 15-3 show rmon event Output Details

Output Field	What It Displays...
Index	Index number for this event entry.
Owner	Text string identifying who configured this entry.
Status	Whether this event entry is enabled (valid) or disabled.
Description	Text string description of this event.
Type	Whether the event notification will be a log entry, and SNMP trap, both, or none.
Community	SNMP community name if message type is set to trap.
Last Time Sent	When an event notification matching this entry was sent.

set rmon event properties

Use this command to configure an RMON event entry, or to create a new event entry with an unused event index number.

Syntax

set rmon event properties *index* [**description** *description*] [**type {none** | **log** | **trap** | **both}**] [**community** *community*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 100. Maximum value is **65535**.
description *description*	(Optional) Specifies a text string description of this event.
type none | **log** | **trap** | **both**	(Optional) Specifies the type of RMON event notification as: none, a log table entry, an SNMP trap, or both a log entry and a trap message.
community *community*	(Optional) Specifies an SNMP community name to use if the message type is set to **trap**. For details on setting SNMP traps and community names, refer to "Creating a Basic SNMP Trap Configuration" on page 8-37.
owner *owner*	(Optional) Specifies the name of the entity that configured this entry.

Defaults

If **description** is not specified, none will be applied.

If not specified, **type none** will be applied.

If *owner* is not specified, **monitor** will be applied.

Mode

Switch command, read-write.

Example

This example shows how to create and enable an RMON event entry called "STP topology change" that will send both a log entry and an SNMP trap message to the "public" community:

```
C3(rw)->set rmon event properties 2 description "STP topology change" type both
community public owner Manager
```

set rmon event status

Use this command to enable an RMON event entry. An event entry describes the parameters of an RMON event that can be triggered. Events can be fired by RMON alarms and can be configured to create a log entry, generate a trap, or both.

Syntax

set rmon event status *index* **enable**

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 100. Maximum value is **65535**.
enable	Enables this event entry.

Defaults

None.

Mode

Switch command, read-write.

Usage

An RMON event entry can be created using this command, configured using the **set rmon event properties** command ("set rmon event properties" on page 15-14), then enabled using this command. An RMON event entry can be created and configured at the same time by specifying an unused index with the **set rmon event properties** command.

Example

This example shows how to enable RMON event entry 1:

```
C3(rw)->set rmon event status 1 enable
```

clear rmon event

Use this command to delete an RMON event entry and any associated log entries.

Syntax

clear rmon event *index*

Parameters

index	Specifies the index number of the entry to be cleared.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear RMON event 1:

```
C3(rw)->clear rmon event 1
```

Filter Group Commands

The packet capture and filter function is disabled by default. Only one interface can be configured for capturing and filtering at a time.

When packet capture is enabled on an interface, the SecureStack C3 switch will capture 100 frames as close to sequentially as possible. These 100 frames will be placed into a buffer for inspection. If there is data in the buffer when the function is started, the buffer will be overwritten. Once 100 frames have been captured, the capture will stop. Filtering will be performed on the frames captured in the buffer. Therefore, only a subset of the frames captured will be available for display.

Note: Packet capture is sampling only and does not guarantee receipt of back to back packets.

One channel at a time can be supported, with up to three filters. Configured channel, filter, and buffer control information will be saved across resets, but captured frames within the buffer will not be saved.

This function cannot be used concurrently with port mirroring. The system will check to prevent concurrently enabling both functions, and a warning will be generated in the CLI if attempted.

Commands

show rmon channel

Use this command to display RMON channel entries for one or more ports.

Syntax

show rmon channel [*port-string*]

Parameters

port-string	(Optional) Displays RMON channel entries for a specific port(s).

Defaults

If *port-string* is not specified, information about all channels will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display RMON channel information for ge.2.12:

```
C3(rw)->show rmon channel ge.2.12
Port ge.2.12    Channel index= 628      EntryStatus= valid
-----------------------------------------------------------
Control             off       AcceptType          matched
OnEventIndex        0         OffEventIndex       0
EventIndex          0         Status              ready
Matches             4498
Description         Thu Dec 16 12:57:32 EST 2004
Owner               NetSight smith
```

set rmon channel

Use this command to configure an RMON channel entry.

Syntax

set rmon channel *index port-string* [**accept** {**matched** | **failed**}] [**control** {**on** | **off**}] [**description** *description*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 2. Maximum value is **65535**.
port-string	Specifies the port on which traffic will be monitored.
accept matched | **failed**	(Optional) Specifies the action of the filters on this channel as: • **matched** - Packets will be accepted on filter matches • **failed** - Packets will be accepted if they fail a match
control on | **off**	(Optional) Enables or disables control of the flow of data through the channel.
description *description*	(Optional) Specifies a description for this channel.
owner *owner*	(Optional) Specifies the name of the entity that configured this entry.

Defaults

If an action is not specified, packets will be accepted on filter matches.

If not specified, **control** will be set to **off**.

If a **description** is not specified, none will be applied.

If *owner* is not specified, it will be set to **monitor.**

Mode

Switch command, read-write.

Example

This example shows how to create an RMON channel entry:

```
C3(rw)->set rmon channel 54313 ge.2.12 accept failed control on description
"capture all"
```

clear rmon channel

Use this command to clear an RMON channel entry.

Syntax

clear rmon channel *index*

Parameters

index	Specifies the channel entry to be cleared.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear RMON channel entry 2:

```
C3(rw)->clear rmon channel 2
```

show rmon filter

Use this command to display one or more RMON filter entries.

Syntax

show rmon filter [**index** *index* | **channel** *channel*]

Parameters

index *index* | **channel** *channel*	(Optional) Displays information about a specific filter entry, or about all filters which belong to a specific channel.

Defaults

If no options are specified, information for all filter entries will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display all RMON filter entries and channel information:

```
C3(rw)->show rmon filter

Index= 55508    Channel Index= 628      EntryStatus= valid
------------------------------------------------------------
Data Offset         0         PktStatus           0
PktStatusMask       0         PktStatusNotMask    0
Owner               ETS,NAC-D
----------------------------
Data
ff ff ff ff ff ff
----------------------------
DataMask
ff ff ff ff ff ff
----------------------------
DataNotMask
00 00 00 00 00 00
```

set rmon filter

Use this command to configure an RMON filter entry.

Syntax

set rmon filter *index channel-index* [**offset** *offset*] [**status** *status*] [**smask** *smask*] [**snotmask** *snotmask*] [**data** *data*] [**dmask** *dmask*] [**dnotmask** *dnotmask*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 10. Maximum value is **65535**.
channel-index	Specifies the channel to which this filter will be applied.
offset *offset*	(Optional) Specifies an offset from the beginning of the packet to look for matches.
status *status*	(Optional) Specifies packet status bits that are to be matched.
smask *smask*	(Optional) Specifies the mask applied to status to indicate which bits are significant.
snotmask *snotmask*	(Optional) Specifies the inversion mask that indicates which bits should be set or not set
data *data*	(Optional) Specifies the data to be matched.
dmask *dmask*	(Optional) Specifies the mask applied to data to indicate which bits are significant.
dnotmask *dnotmask*	(Optional) Specifies the inversion mask that indicates which bits should be set or not set.
owner	(Optional) Specifies the name of the entity that configured this entry.

Defaults

If *owner* is not specified, it will be set to **monitor.**

If no other options are specified, none (0) will be applied.

Mode

Switch command, read-write.

Example

This example shows how to create RMON filter 1 and apply it to channel 9:

```
C3(rw)->set rmon filter 1 9 offset 30 data 0a154305 dmask ffffffff
```

clear rmon filter

Use this command to clear an RMON filter entry.

Syntax

clear rmon filter {**index** *index* | **channel** *channel*}

Parameters

index *index* | **channel** *channel*	Clears a specific filter entry, or all entries belonging to a specific channel.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear RMON filter entry 1:

```
C3(rw)->clear rmon filter index 1
```

Packet Capture Commands

Note that packet capture filter is sampling only and does not guarantee receipt of back-to-back packets.

Purpose

To display RMON capture entries, configure, enable, or disable capture entries, and clear capture entries.

Commands

For information about...	Refer to page...
show rmon capture	15-22
set rmon capture	15-23
clear rmon capture	15-24

show rmon capture

Use this command to display RMON capture entries and associated buffer control entries.

Syntax

show rmon capture [*index* [**nodata**]]

Parameters

index	(Optional) Displays the specified buffer control entry and all captured packets associated with that entry.
nodata	(Optional) Displays only the buffer control entry specified by index.

Defaults

If no options are specified, all buffer control entries and associated captured packets will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display RMON capture entries and associated buffer entries:

```
C3(rw)->show rmon capture

Buf.control= 28062  Channel= 38283      EntryStatus= valid
------------------------------------------------------------
FullStatus          avail     FullAction          lock
Captured packets    251       Capture slice       1518
Download size       100       Download offset     0
Max Octet Requested 50000     Max Octet Granted   50000
Start time          1 days 0 hours 51 minutes 15 seconds
```

```
Owner               monitor


captureEntry= 1        Buff.control= 28062
-----------------------------------------
Pkt ID      9          Pkt time    1 days 0 hours 51 minutes 15 seconds
Pkt Length  93         Pkt status  0
Data:
00 00 5e 00 01 01 00 01 f4 00 7d ce 08 00 45 00
00 4b b4 b9 00 00 40 11 32 5c 0a 15 43 05 86 8d
bf e5 00 a1 0e 2b 00 37 cf ca 30 2d 02 01 00 04
06 70 75 62 6c 69 63 a2 20 02 02 0c 92 02 01 00
02 01 00 30 14 30 12 06 0d 2b 06 01 02 01 10 07
01 01 0b 81 fd 1c 02 01 01 00 11 0b 00
```

set rmon capture

Use this command to configure an RMON capture entry.

Syntax

set rmon capture *index* {*channel* [**action** {**lock**}] [**slice** *slice*] [**loadsize** *loadsize*] [**offset** *offset*] [**asksize** *asksize*] [**owner** *owner*]}

Parameters

index	Specifies a buffer control entry.
channel	Specifies the channel to which this capture entry will be applied.
action lock	(Optional) Specifies the action of the buffer when it is full as: • **lock** - Packets will cease to be accepted
slice *slice*	(Optional) Specifies the maximum octets from each packet to be saved in a buffer. Currently, the only value allowed is 1518.
loadsize *loadsize*	(Optional) Specifies the maximum octets from each packet to be downloaded from the buffer. The default is 100.
offset *offset*	(Optional) Specifies the first octet from each packet that will be retrieved.
asksize *asksize*	(Optional) Specifies the requested maximum octets to be saved in this buffer. Currently, the only value accepted is -1, which requests as many octets as possible.
owner	(Optional) Specifies the name of the entity that configured this entry.

Defaults

If not specified, **action** defaults to **lock**.

If not specified, **offset** defaults to **0**.

If not specified, **asksize** defaults to -**1** (which will request as many octets as possible).

If **slice** is not specified, **1518** will be applied.

If **loadsize** is not specified, **100** will be applied.

If *owner* is not specified, it will be set to **monitor**.

Mode

Switch command, read-write.

Example

This example shows how to create RMON capture entry 1 to “listen” on channel 628:

```
C3(rw)->set rmon capture 1 628
```

clear rmon capture

Use this command to clears an RMON capture entry.

Syntax

clear rmon capture *index*

Parameters

index	Specifies the capture entry to be cleared.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear RMON capture entry 1:

```
C3(rw)->clear rmon capture 1
```

16

DHCP Server Configuration

This chapter describes the commands to configure the IPv4 DHCP server functionality on a SecureStack C3 switch.

DHCP Overview

Dynamic Host Configuration Protocol (DHCP) for IPv4 is a network layer protocol that implements automatic or manual assignment of IP addresses and other configuration information to client devices by servers. A DHCP server manages a user-configured pool of IP addresses from which it can make assignments upon client requests. A relay agent passes DHCP messages between clients and servers which are on different physical subnets.

DHCP Relay Agent

The DHCP/BOOTP relay agent function can be configured on all of the SecureStack C3's routing interfaces. The relay agent can forward a DHCP client's request to a DHCP server located on a different network if the address of the server is configured as a helper address on the receiving interface. The relay agent interface must be a VLAN which is configured with an IP address. Refer to the **ip helper-address** command ("ip helper-address" on page 19-18) for more information.

DHCP Server

DHCP server functionality allows the SecureStack C3 switch to provide basic IP configuration information to a client on the network who requests such information using the DHCP protocol.

DHCP provides the following mechanisms for IP address allocation by a DHCP server:

- Automatic—DHCP server assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address) from a defined pool of IP addresses configured on the server.
- Manual—A client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client. This is managed by means of "static" address pools configured on the server.

The amount of time that a particular IP address is valid for a system is called a lease. The SecureStack C3 maintains a lease database which contains information about each assigned IP

address, the MAC address to which it is assigned, the lease expiration, and whether the address assignment is dynamic (automatic) or static (manual). The DHCP lease database is stored in flash memory.

In addition to assigning IP addresses, the DHCP server can also be configured to assign the following to requesting clients:

- Default router(s)
- DNS server(s) and domain name
- NetBIOS WINS server(s) and node name
- Boot file
- DHCP options as defined by RFC 2132

Note: A total of 16 address pools, dynamic and/or static, and a maximum of 256 addresses for the entire switch, can be configured on the SecureStack C3.

Configuring a DHCP Server

For DHCP to function on SecureStack C3 systems, the system has to "know about" the IP network for which the DHCP pool is to be created.

On the C3, there are two ways to configure a DHCP server: one is to associate the DHCP address pool with the switch's host port IP address, and the other is to associate the DHCP address pool with a routed interface.

Since on a C3 system, the host port IP address cannot fall within a configured routed interface on the system, a typical C3 system configured with routing interfaces will not have a host port IP address. Therefore, all DHCP pools would be associated with routed interfaces.

The following tasks provide basic DHCP server functionality when the DHCP pool is associated with the system's host IP address. This procedure would typically be used when the C3 system is NOT configured for routing.

1. Configure the system (stack) host port IP address with the **set ip address** command. Once the system's IP address is configured, the system then "knows" about the configured subnet. For example:

   ```
   set ip address 192.0.0.50 mask 255.255.255.0
   ```

2. Enable DHCP server functionality on the system with the **set dhcp enable** command.

3. Configure an IP address pool for dynamic IP address assignment. The only *required* steps are to name the pool and define the network number and mask for the pool. Note that the pool has to be in the same subnet and use the same mask as the system host port IP address. For example:

   ```
   set dhcp pool auto-pool network 192.0.0.0 255.255.255.0
   ```

   All DHCP clients served by this switch must be in the same VLAN as the system's host port.

The following tasks provide basic DHCP server functionality when the DHCP pool is associated with a routed interface.

1. Create a VLAN and add ports to the VLAN. Only DHCP clients associated with this VLAN will be served IP addresses from the DHCP address pool associated with this routed interface (VLAN). In this example, VLAN 6 is created and ports ge.1.1 through ge.1.10 are added to VLAN 6:

   ```
   set vlan create 6
   ```

```
set port vlan ge.1.1-10 6
```

2. Create a routed interface for the VLAN in router configuration mode. In the following example, an IP address is associated with routed interface VLAN 6:

   In router configuration mode:

   ```
   interface vlan 6
   no shutdown
   ip address 6.6.1.1 255.255.0.0
   ```

3. Enable DHCP server functionality on the system with the **set dhcp enable** command.

4. Create the DHCP address pool. The only *required* steps are to name the pool and define the network number and mask for the pool. Note that the pool has to be in the same subnet as the routed interface and use the same mask configured on the routed interface. For example:

   ```
   set dhcp pool auto-pool network 6.6.0.0 255.255.0.0
   ```

   DHCP clients in VLAN 6 will be served IP addresses from this DHCP address pool.

Optional DHCP server tasks include:

- You can limit the scope of addresses assigned to a pool for dynamic address assignment with the **set dhcp exclude** command. Up to 128 non-overlapping address ranges can be excluded on the SecureStack C3. For example:

  ```
  set dhcp exclude 192.0.0.1 192.0.0.10
  ```

  Note: The IP address of the system's host port or the routed interface is automatically excluded.

- Configure static address pools for manual address assignment. The only *required* steps are to name the pool, configure either the hardware address of the client or the client identifier, and configure the IP address and mask for the manual binding. For example:

  ```
  set dhcp pool static-pool hardware-address 0011.2233.4455
  set dhcp pool static-pool host 192.0.0.200 255.255.255.0
  ```

- Set other DHCP server parameters such as the number of ping packets to be sent before assigning an IP address, or enabling conflict logging.

Configuring General DHCP Server Parameters

Purpose

To configure DHCP server parameters, and to display and clear address binding information, server statistics, and conflict information.

Commands

For information about...	Refer to page...
set dhcp	16-4
set dhcp bootp	16-4
set dhcp conflict logging	16-5
show dhcp conflict	16-5

set dhcp

Use this command to enable or disable the DHCP server functionality on the SecureStack C3.

Syntax

set dhcp {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables DHCP server functionality. By default, DHCP server is disabled.

Defaults

None.

Mode

Switch command, read-write.

Example

This example enables DHCP server functionality.

```
C3(rw)->set dhcp enable
```

set dhcp bootp

Use this command to enable or disable automatic address allocation for BOOTP clients. By default, address allocation for BOOTP clients is disabled. Refer to RFC 1534, “Interoperation Between DHCP and BOOTP,” for more information.

Syntax

set dhcp bootp {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables address allocation for BOOTP clients.

Defaults

None.

Mode

Switch command, read-write.

Example

This example enables address allocation for BOOTP clients.

```
C3(rw)->set dhcp bootp enable
```

set dhcp conflict logging

Use this command to enable conflict logging. By default, conflict logging is enabled. Use the **clear dhcp conflict logging** command to disable conflict logging.

Syntax

set dhcp conflict logging

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example enables DHCP conflict logging.

```
C3(rw)->set dhcp conflict logging
```

show dhcp conflict

Use this command to display conflict information, for one address or all addresses.

Syntax

show dhcp conflict [*address*]

Parameters

address	[Optional] Specifies the address for which to display conflict information.

Defaults

If no address is specified, conflict information for all addresses is displayed.

Mode

Read-only.

Example

This example displays conflict information for all addresses. Note that ping is the only detection method used.

```
C3(ro)->show dhcp conflict

IP address          Detection Method          Detection Time
-----------         -----------------         --------------
192.0.0.2           Ping                      0 days 19h:01m:23s
192.0.0.3           Ping                      0 days 19h:00m:46s
192.0.0.4           Ping                      0 days 19h:01m:25s
192.0.0.12          Ping                      0 days 19h:01m:26s
```

clear dhcp conflict

Use this command to clear conflict information for one or all addresses, or to disable conflict logging.

Syntax

clear dhcp conflict {**logging** | *ip-address*| ***}**

Parameters

logging	Disables conflict logging.
ip-address	Clears the conflict information for the specified IP address.
*	Clears the conflict information for all IP addresses.

Defaults

None.

Mode

Switch command, read-write.

Examples

This example disables DHCP conflict logging.

```
C3(rw)->clear dhcp conflict logging
```

This example clears the conflict information for the IP address 192.0.0.2.

```
C3(rw)->clear dhcp conflict 192.0.0.2
```

set dhcp exclude

Use this command to configure the IP addresses that the DHCP server should not assign to DHCP clients. Multiple address ranges can be configured but the ranges cannot overlap. Up to 128 non-overlapping address ranges can be excluded.

Syntax

set dhcp exclude *low-ipaddr* [*high-ipaddr*]

Parameters

low-ipaddr	Specifies the first IP address in the address range to be excluded from assignment.
high-ipaddr	(Optional) Specifies the last IP address in the address range to be excluded.

Defaults

None.

Mode

Switch command, read-write.

Example

This example first configures the address pool named "auto1" with 255 addresses for the Class C network 172,20.28.0, with the **set dhcp pool network** command. Then, the example limits the scope of the addresses that can be assigned by a DHCP server by excluding addresses 172.20.28.80 – 100, with the **set dhcp exclude** command.

```
C3(rw)->set dhcp pool auto1 network 172.20.28.0 24
C3(rw)->set dhcp exclude 172.20.28.80 172.20.28.100
```

clear dhcp exclude

Use this command to clear the configured IP addresses that the DHCP server should not assign to DHCP clients.

Syntax

clear dhcp exclude *low-ipaddr* [*high-ipaddr*]

Parameters

low-ipaddr	Specifies the first IP address in the address range to be cleared.
high-ipaddr	(Optional) Specifies the last IP address in the address range to be cleared.

Defaults

None.

Mode

Switch command, read-write.

Example

This example clears the previously excluded range of IP addresses between 192.168.1.88 through 192.168.1.100.

```
C3(rw)->clear dhcp exclude 192.168.1.88 192.168.1.100
```

set dhcp ping

Use this command to configure the number of ping packets the DHCP server sends to an IP address before assigning the address to a requesting client.

Syntax

set dhcp ping packets *number*

Parameters

packets *number*	Specifies the number of ping packets to be sent. The value of number can be 0, or range from 2 to 10. Entering 0 disables this function. The default value is 2 packets.

Defaults

None.

Mode

Switch command, read-write.

Example

This example sets the number of ping packets sent to 3.

```
C3(rw)->set dhcp ping packets 3
```

clear dhcp ping

Use this command to reset the number of ping packets sent by the DHCP server back to the default value of 2.

Syntax

clear dhcp ping packets

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example resets the number of ping packets sent back to the default value.

```
C3(rw)->clear dhcp ping packets
```

show dhcp binding

Use this command to display binding information for one or all IP addresses.

Syntax

show dhcp binding [*ip-address*]

Parameters

ip-address	(Optional) Specifies the IP address for which to display binding information.

Defaults

If no IP address is specified, binding information for all addresses is displayed.

Mode

Read-only.

Example

This example displays binding information about all addresses.

```
C3(rw)->show dhcp binding
IP address         Hardware Address     Lease Expiration     Type
-----------        -----------------    -----------------    -----
192.0.0.6          00:33:44:56:22:39    00:11:02             Automatic
192.0.0.8          00:33:44:56:22:33    00:10:22             Automatic
192.0.0.10         00:33:44:56:22:34    00:09:11             Automatic
192.0.0.11         00:33:44:56:22:35    00:10:05             Automatic
192.0.0.12         00:33:44:56:22:36    00:10:30             Automatic
192.0.0.13         00:33:44:56:22:37    infinite             Manual
192.0.0.14         00:33:44:56:22:38    infinite             Manual
```

clear dhcp binding

Use this command to clear (delete) one or all DHCP address bindings.

Syntax

clear dhcp binding {*ip-addr* | ***}

Parameters

ip-addr	Specifies the IP address for which to clear/delete the DHCP binding.
*	Deletes all address bindings.

Defaults

None.

Mode

Switch command, read-write.

Example

This example deletes the DHCP address binding for IP address 192.168.1.1.

```
C3(rw)->clear dhcp binding 192.168.1.1
```

show dhcp server statistics

Use this command to display DHCP server statistics.

Syntax

show dhcp server statistics

Parameters

None.

Defaults

None.

Mode

Read-only.

Example

This example displays server statistics.

```
C3(ro)->show dhcp server statistics

Automatic Bindings                          36
Expired Bindings                            6
Malformed Bindings                          0
Messages                                 Received
----------                              ----------
DHCP DISCOVER                               382
DHCP REQUEST                                3855
DHCP DECLINE                                0
DHCP RELEASE                                67
DHCP INFORM                                 1

Messages                                   Sent
----------                                 ------
DHCP OFFER                                  381
DHCP ACK                                    727
DHCP NACK                                   2
```

clear dhcp server statistics

Use this command to clear all DHCP server counters.

Syntax

clear dhcp server statistics

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example clears all DHCP server counters.

```
C3(rw)->clear dhcp server statistics
```

Configuring IP Address Pools

Manual Pool Configuration Considerations

- The subnet of the IP address being issued should be on the same subnet as the ingress interface (that is, the subnet of the host IP address of the switch, or if routing interfaces are configured, the subnet of the routing interface).
- A manual pool can be configured using either the client's hardware address (**set dhcp pool hardware-address**) or the client's client-identifier (**set dhcp pool client-identifier**), but using both is not recommended.
- If the incoming DHCP request packet contains a client-identifier, then a manual pool configured with that client-identifier must exist on the switch in order for the request to be processed. The hardware address is not checked.
- A hardware address and type (Ethernet or IEEE 802) configured in a manual pool is checked only when a client-identifier is not also configured for the pool and the incoming DHCP request packet does not include a client-identifier option.

Purpose

To configure and clear DHCP address pool parameters, and to display address pool configuration information.

Note: A total of 16 address pools, dynamic and/or static, can be configured on the SecureStack C3.

Commands

For information about...	Refer to page...
set dhcp pool	16-13
clear dhcp pool	16-14
set dhcp pool network	16-14
clear dhcp pool network	16-15
set dhcp pool hardware-address	16-15
clear dhcp pool hardware-address	16-16
set dhcp pool host	16-16
clear dhcp pool host	16-17
set dhcp pool client-identifier	16-17
clear dhcp pool client-identifier	16-18
set dhcp pool client-name	16-19
clear dhcp pool client-name	16-19
set dhcp pool bootfile	16-20
clear dhcp pool bootfile	16-20

set dhcp pool

Use this command to create and assign a name to a DHCP server pool of addresses. Up to 16 address pools may be configured on a SecureStack C3. Note that entering this command is not required to create an address pool before configuring other address pool parameters.

Syntax

`set dhcp pool` *`poolname`*

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example creates an address pool named “auto1.”

```
C3(rw)->set dhcp pool auto1
```

clear dhcp pool

Use this command to delete a DHCP server pool of addresses.

Syntax

clear dhcp pool *poolname*

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example deletes the address pool named "auto1."

```
C3(rw)->clear dhcp pool auto1
```

set dhcp pool network

Use this command to configure the subnet number and mask for an automatic DHCP address pool.

Syntax

set dhcp pool *poolname* **network** *number* {*mask* | *prefix-length*}

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
number	Specifies an IP subnet for the address pool.
mask	Specifies the subnet mask in dotted quad notation.
prefix-length	Specifies the subnet mask as an integer.

Defaults

None.

Mode

Switch command, read-write.

Usage

Use this command to configure a set of IP addresses to be assigned by the DHCP server using the specified address pool. In order to limit the scope of the addresses configured with this command, use the set dhcp exclude command on page 16-7.

Examples

This example configures the IP subnet 172.20.28.0 with a prefix length of 24 for the automatic DHCP pool named "auto1." Alternatively, the mask could have been specified as 255.255.255.0.

```
C3(rw)->set dhcp pool auto1 network 172.20.28.0 24
```

This example limits the scope of 255 addresses created for the Class C network 172,20.28.0 by the previous example, by excluding addresses 172.20.28.80 – 100.

```
C3(rw)->set dhcp exclude 172.20.28.80 172.20.28.100
```

clear dhcp pool network

Use this command to remove the network number and mask of a DHCP server pool of addresses.

Syntax

clear dhcp pool *poolname* **network**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example deletes the network and mask from the address pool named "auto1."

```
C3(rw)->clear dhcp pool auto1 network
```

set dhcp pool hardware-address

Use this command to configure the MAC address of the DHCP client and create an address pool for manual binding. You can use either this command or the **set dhcp pool client-identifier** command to create a manual binding pool, but using both is not recommended.

Syntax

set dhcp pool *poolname* **hardware-address** *hw-addr* [*type*]

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
hw-addr	Specifies the MAC address of the client's hardware platform. This value can be entered using dotted hexadecimal notation or colons.
type	(Optional) Specifies the protocol of the hardware platform. Valid values are 1 for Ethernet or 6 for IEEE 802. Default value is 1, Ethernet.

Defaults

If no *type* is specified, Ethernet is assumed.

Mode

Switch command, read-write.

Example

This example specifies 0001.f401.2710 as the Ethernet MAC address for the manual address pool named "manual1." Alternatively, the MAC address could have be entered as 00:01:f4:01:27:10.

```
C3(rw)->set dhcp pool manual1 hardware-address 0001.f401.2710
```

clear dhcp pool hardware-address

Use this command to remove the hardware address of a DHCP client from a manual binding address pool.

Syntax

clear dhcp pool *poolname* **hardware-address**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example deletes the client hardware address from the address pool named "manual1."

```
C3(rw)->clear dhcp pool manual1 hardware-address
```

set dhcp pool host

Use this command to configure an IP address and network mask for a manual DHCP binding.

Syntax

set dhcp pool *poolname* **host** *ip-address* [*mask* | *prefix-length*]

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
ip-address	Specifies the IP address for manual binding.

mask	(Optional) Specifies the subnet mask in dotted quad notation.
prefix-length	(Optional) Specifies the subnet mask as an integer.

Defaults

If a mask or prefix is not specified, the class A, B, or C natural mask will be used.

Mode

Switch command, read-write.

Example

This example shows how to configure the minimum requirements for a manual binding address pool. First, the hardware address of the client's hardware platform is configured, followed by configuration of the address to be assigned to that client manually.

```
C3(rw)->set dhcp pool manual1 hardware-address 0001.f401.2710
C3(rw)->set dhcp pool manual1 host 15.12.1.99 255.255.248.0
```

clear dhcp pool host

Use this command to remove the host IP address from a manual binding address pool.

Syntax

clear dhcp pool *poolname* **host**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example deletes the host IP address from the address pool named "manual1."

```
C3(rw)->clear dhcp pool manual1 host
```

set dhcp pool client-identifier

Use this command to configure the client identifier of the DHCP client and create an address pool for manual binding. You can use either this command or the **set dhcp pool hardware-address** command to create a manual binding pool, but using both is not recommended.

Syntax

set dhcp pool *poolname* **client-identifier** *id*

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
id	Specifies the unique client identifier for this client. The value must be entered in xx:xx:xx:xx:xx:xx format.

Defaults

None.

Mode

Switch command, read-write.

Usage

The client identifier is formed by concatenating the media type and the MAC address. For example, if the client hardware type is Ethernet and the client MAC address is 00:01:22:33:44:55, then the client identifier configured with this command must be 01:00:01:22:33:44:55.

Example

This example shows how to configure the minimum requirements for a manual binding address pool, using a client identifier rather than the hardware address of the client's hardware platform.

```
C3(rw)->set dhcp pool manual2 client-identifier 01:00:01:22:33:44:55
C3(rw)->set dhcp pool manual2 host 10.12.1.10 255.255.255.0
```

clear dhcp pool client-identifier

Use this command to remove the unique identifier of a DHCP client from a manual binding address pool.

Syntax

clear dhcp pool *poolname* **client-identifier**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example deletes the client identifier from the address pool named "manual1."

```
C3(rw)->clear dhcp pool manual1 client-identifier
```

set dhcp pool client-name

Use this command to assign a name to a DHCP client when creating an address pool for manual binding.

Syntax

set dhcp pool *poolname* **client-name** *name*

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
name	Specifies the name to be assigned to this client. Client names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example configures the client name "appsvr1" to the manual binding pool "manual2."

```
C3(rw)->set dhcp pool manual2 client-identifier 01:22:33:44:55:66
C3(rw)->set dhcp pool manual2 host 10.12.1.10 255.255.255.0
C3(rw)->set dhcp pool manual2 client-name appsvr1
```

clear dhcp pool client-name

Use this command to delete a DHCP client name from an address pool for manual binding.

Syntax

clear dhcp pool *poolname* **client-name**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example deletes the client name from the manual binding pool "manual2."

```
C3(rw)->clear dhcp pool manual2 client-name
```

set dhcp pool bootfile

Use this command to specify a default boot image for the DHCP clients who will be served by the address pool being configured.

Syntax

set dhcp pool *poolname* **bootfile** *filename*

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
filename	Specifies the boot image file name.

Defaults

None.

Mode

Switch command, read-write.

Example

This example sets the boot image filename for address pool named "auto1."

```
C3(rw)->set dhcp pool auto1 bootfile image1.img
```

clear dhcp pool bootfile

Use this command to remove a default boot image from the address pool being configured.

Syntax

clear dhcp pool *poolname* **bootfile**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example removes the boot image filename from address pool named "auto1."

```
C3(rw)->clear dhcp pool auto1 bootfile
```

set dhcp pool next-server

Use this command to specify the file server from which the default boot image is to be loaded by the client.

Syntax

set dhcp pool *poolname* **next-server** *ip-address*

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
ip-address	Specifies the IP address of the file server the DHCP client should contact to load the default boot image.

Defaults

None.

Mode

Switch command, read-write.

Example

This example specifies the file server from which clients being served by address pool "auto1" should download the boot image file "image1.img."

```
C3(rw)->set dhcp pool auto1 bootfile image1.img
C3(rw)->set dhcp pool auto1 next-server 10.1.1.10
```

clear dhcp pool next-server

Use this command to remove the boot image file server from the address pool being configured.

Syntax

clear dhcp pool *poolname* **next-server**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example removes the file server from address pool "auto1."

```
C3(rw)->clear dhcp pool auto1 next-server
```

set dhcp pool lease

Use this command to specify the duration of the lease for an IP address assigned by the DHCP server from the address pool being configured.

Syntax

set dhcp pool *poolname* **lease** {*days* [*hours* [*minutes*]] | **infinite**}

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
days	Specifies the number of days an address lease will remain valid. Value can range from 0 to 59.
hours	(Optional) When a *days* value has been assigned, specifies the number of hours an address lease will remain valid. Value can range from 0 to 1439.
minutes	(Optional) When a *days* value and an *hours* value have been assigned, specifies the number of minute an address lease will remain valid. Value can range from 0 to 86399.
infinite	Specifies that the duration of the lease will be unlimited.

Defaults

If no lease time is specified, a lease duration of 1 day is configured.

Mode

Switch command, read-write.

Example

This example configures a lease duration of 12 hours for the address pool being configured. Note that to configure a lease time less than one day, enter 0 for days, then the number of hours and minutes.

```
C3(rw)->set dhcp pool auto1 lease 0 12
```

clear dhcp pool lease

Use this command to restore the default lease time value of one day for the address pool being configured.

Syntax

clear dhcp pool *poolname* **lease**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

Clears the lease time for this address pool to the default value of one day.

Mode

Switch command, read-write.

Example

This example restores the default lease duration of one day for address pool "auto1."

```
C3(rw)->clear dhcp pool auto1 lease
```

set dhcp pool default-router

Use this command to specify a default router list for the DHCP clients served by the address pool being configured. Up to 8 default routers can be configured.

Syntax

set dhcp pool *poolname* **default-router** *address* [*address2 ... address8*]

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
address	Specifies the IP address of a default router.
address2 ... address8	(Optional) Specifies, in order of preference, up to 7 additional default router addresses.

Defaults

None.

Mode

Switch command, read-write.

Example

This example assigns a default router at 10.10.10.1 to the address pool named "auto1."

```
C3(rw)->set dhcp pool auto1 default-router 10.10.10.1
```

clear dhcp pool default-router

Use this command to delete the default routers configured for this address pool.

Syntax

clear dhcp pool *poolname* **default-router**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example removes the default router from the address pool "auto1."

```
C3(rw)->clear dhcp pool auto1 default-router
```

set dhcp pool dns-server

Use this command to specify one or more DNS servers for the DHCP clients served by the address pool being configured. Up to 8 DNS servers can be configured.

Syntax

set dhcp pool *poolname* **dns-server** *address* [*address2 ... address8*]

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
address	Specifies the IP address of a DNS server.
address2 ... address8	(Optional) Specifies, in order of preference, up to 7 additional DNS server addresses.

Defaults

None.

Mode

Switch command, read-write.

Example

This example assigns a DNS server at 10.14.10.1 to the address pool "'auto1."

```
C3(rw)->set dhcp pool auto1 dns-server 10.14.10.1
```

clear dhcp pool dns-server

Use this command to remove the DNS server list from the address pool being configured.

Syntax

clear dhcp pool *poolname* **dns-server**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example removes the DNS server list from the address pool "auto1."

```
C3(rw)->clear dhcp pool auto1 dns-server
```

set dhcp pool domain-name

Use this command to specify a domain name to be assigned to DHCP clients served by the address pool being configured.

Syntax

set dhcp pool *poolname* **domain-name** *domain*

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
domain	Specifies the domain name string. The domain name can be up to 255 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example assigns the "mycompany.com" domain name to the address pool "auto1."

```
C3(rw)->set dhcp pool auto1 domain-name mycompany.com
```

clear dhcp pool domain-name

Use this command to remove the domain name from the address pool being configured.

Syntax

clear dhcp pool *poolname* **domain-name**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example removes the domain name from the address pool "auto1."

```
C3(rw)->clear dhcp pool auto1 domain-name
```

set dhcp pool netbios-name-server

Use this command to assign one or more NetBIOS name servers for the DHCP clients served by the address pool being configured. Up to 8 NetBIOS name servers can be configured.

Syntax

set dhcp pool *poolname* **netbios-name-server** *address* [*address2 ... address8*]

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
address	Specifies the IP address of a NetBIOS name server.
address2 ... address8	(Optional) Specifies, in order of preference, up to 7 additional NetBIOS name server addresses.

Defaults

None.

Mode

Switch command, read-write.

Example

This example assigns a NetBIOS name server at 10.15.10.1 to the address pool being configured.

```
C3(rw)->set dhcp pool auto1 netbios-name-server 10.15.10.1
```

clear dhcp pool netbios-name-server

Use this command to remove the NetBIOS namer server list from the address pool being configured.

clear dhcp pool *poolname* **netbios-name-server**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example removes the NetBIOS name server list from the address pool auto1.

```
C3(rw)->clear dhcp pool auto1 netbios-name-server
```

set dhcp pool netbios-node-type

Use this command to specify a NetBIOS node (server) type for the DHCP clients served by the address pool being configured.

Syntax

set dhcp pool *poolname* **netbios-node-type** {**b-node | h-node | p-node | m-node**}

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
b-node	Specifies the NetBIOs node type to be broadcast (no WINS).
h-node	Specifies the NetBIOs node type to be hybrid (WINS, then broadcast).
p-node	Specifies the NetBIOs node type to be peer (WINS only).
m-node	Specifies the NetBIOs node type to be mixed (broadcast, then WINS).

Defaults

None.

Mode

Switch command, read-write.

Example

This example specifies hybrid as the NetBIOS node type for the address pool “auto1.”

```
C3(rw)->set dhcp pool auto1 netbios-node-type h-node
```

clear dhcp pool netbios-node-type

Use this command to remove the NetBIOS node type from the address pool being configured.

Syntax

clear dhcp pool *poolname* **netbios-node-type**

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Switch command, read-write.

Example

This example removes the NetBIOS node type from the address pool "auto1."

```
C3(rw)->clear dhcp pool auto1 netbios-node-type
```

set dhcp pool option

Use this command to configure DHCP options, described in RFC 2132.

Syntax

set dhcp pool *poolname* **option** *code* {**ascii** *string* | **hex** *string-list* | **ip** *address-list*}

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
code	Specifies the DHCP option code, as defined in RFC 2132. Value can range from 1 to 254.
ascii *string*	Specifies the data in ASCII format. An ASCII character string containing a space must be enclosed in quotations.
hex *string-list*	Specifies the data in HEX format. Up to 8 HEX strings can be entered.
ip *address-list*	Specifies the data in IP address format. Up to 8 IP addresses can be entered.

Defaults

None.

Mode

Switch command, read-write.

Examples

This example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. In this case, IP forwarding is enabled with the 01 value.

```
C3(rw)->set dhcp pool auto1 option 19 hex 01
```

This example configures DHCP option 72, which assigns one or more Web servers for DHCP clients. In this case, two Web server addresses are configured.

```
C3(rw)->set dhcp pool auto1 option 72 ip 168.24.3.252 168.24.3.253
```

clear dhcp pool option

Use this command to remove a DHCP option from the address pool being configured.

Syntax

clear dhcp pool *poolname* **option** *code*

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.
code	Specifies the DHCP option code, as defined in RFC 2132. Value can range from 1 to 254.

Defaults

None.

Mode

Switch command, read-write.

Example

This example removes option 19 from address pool "auto1."

```
C3(rw)->clear dhcp pool auto1 option 19
```

show dhcp pool configuration

Use this command to display configuration information for one or all address pools.

Syntax

show dhcp pool configuration {*poolname* | **all**}

Parameters

poolname	Specifies the name of the address pool. Pool names may be up to 31 characters in length.

Defaults

None.

Mode

Read-only.

Example

This example displays configuration information for all address pools.

```
C3(rw)->show dhcp pool configuration all

Pool: Atg_Pool
Pool Type                                        Dynamic
```

```
Network                                 192.0.0.0 255.255.255.0
Lease Time                              1 days 0 hrs 0 mins
Default Routers                         192.0.0.1

Pool: static1
Pool Type                               Manual
Client Name                             appsvr1
Client Identifier                       01:00:01:f4:01:27:10
Host                                    10.1.1.1 255.0.0.0
Lease Time                              infinite
Option                                  19 hex 01

Pool: static2
Pool Type                               Manual
Hardware Address                        00:01:f4:01:27:10
Hardware Address Type                   ieee802
Host                                    192.168.10.1 255.255.255.0
Lease Time                              infinite
```

17

DHCP Snooping and Dynamic ARP Inspection

This chapter describes two security features:

- DHCP snooping, which monitors DHCP messages between a DHCP client and DHCP server to filter harmful DHCP messages and to build a database of authorized address bindings
- Dynamic ARP inspection, which uses the bindings database created by the DHCP snooping feature to reject invalid and malicious ARP packets

DHCP Snooping Overview

DHCP snooping monitors DHCP messages between DHCP clients and DHCP servers to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are considered authorized.

DHCP snooping is disabled globally and on all VLANs by default. Ports are untrusted by default. DHCP snooping must be enabled globally and on specific VLANs. Ports within the VLANs must be configured as trusted or untrusted. DHCP servers must be reached through trusted ports.

DHCP snooping enforces the following security rules:

- DHCP packets from a DHCP server (DHCP OFFER, DHCP ACK, DHCP NAK) are dropped if received on an untrusted port.
- DHCP RELEASE and DHCP DECLINE messages are dropped if they are for a MAC address in the snooping database but the binding's interface in the database is different from the interface where the message was received.
- On untrusted interfaces, the switch drops DHCP packets whose source MAC address does not match the client hardware address. This feature is a configurable option.

DHCP Message Processing

The hardware identifies all incoming DHCP packets on ports where DHCP snooping is enabled. On untrusted ports, the hardware traps all incoming DHCP packets to the CPU. On trusted ports,

the hardware forwards client messages and copies server messages to the CPU so DHCP snooping can learn the binding.

The DHCP snooping application processes incoming DHCP messages. For DHCP RELEASE and DHCP DECLINE messages, the application compares the receive interface and VLAN with the client's interface and VLAN in the bindings database. If the interfaces do not match, the application logs the event and drops the message. For valid client messages, DHCP snooping compares the source MAC address to the DHCP client hardware address. Where there is a mismatch, DHCP snooping logs and drops the packet. You can disable this feature using the **set dhcpsnooping verify mac-address disable** command.

Note: If the switch has been configured as a DHCP relay agent, to forward client requests to a DHCP server that does not reside on the same broadcast domain as the client, MAC address verification should be disabled in order to allow DHCP RELEASE packets to be processed by the DHCP snooping functionality and client bindings removed from the bindings database.

DHCP snooping can be configured on switching VLANs and routing VLANs. When a DHCP packet is received on a routing VLAN, the DHCP snooping application applies its filtering rules and updates the bindings database. If a client message passes filtering rules, the message is placed into the software forwarding path, where it may be processed by the DHCP relay agent, the local DHCP server, or forwarded as an IP packet.

DHCP snooping forwards valid DHCP client messages received on non-routing VLANs. The message is forwarded on all trusted interfaces in the VLAN. If a DHCP relay agent or local DHCP server co-exist with the DHCP snooping feature, DHCP client messages will be sent to the DHCP relay agent or local DHCP server to process further.

The DHCP snooping application does not forward server messages since they are forwarded in hardware.

Building and Maintaining the Database

The DHCP snooping application uses DHCP messages to build and maintain the bindings database. The bindings database includes only data for clients on untrusted ports. The bindings database includes the following information for each entry:

- Client MAC address
- Client IP address
- Time when client's lease expires
- Client VLAN ID
- Client port

DHCP snooping creates a tentative binding from DHCP DISCOVER and REQUEST messages. Tentative bindings tie a client to a port (the port where the DHCP client message was received). Tentative bindings are completed when DHCP snooping learns the client's IP address from a DHCP ACK message on a trusted port. DHCP snooping removes bindings in response to DECLINE, RELEASE, and NACK messages. The DHCP snooping application ignores the ACK messages sent in reply to the DHCP Inform messages received on trusted ports. You can also enter static bindings into the bindings database.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database.

If the absolute lease time of a snooping database entry expires, then that entry will be removed. Care should be taken to ensure that system time is consistent across the reboots. Otherwise, snooping entries will not expire properly. If a host sends a DHCP RELEASE message while the

switch is rebooting, when the switch receives a DHCP DISCOVERY or REQUEST message, the client's binding will go to a tentative binding state.

Rate Limiting

To protect the switch against DHCP attacks when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds a configurable limit, DHCP snooping brings down the interface. Use the **set port enable** command to re-enable the interface. Both the rate and the burst interval can be configured.

Basic Configuration

The following configuration procedure does not change the write delay to the snooping database or any of the default rate limiting values. Additional configuration notes follow this procedure.

Procedure 17-1 Basic Configuration for DHCP Snooping

Step	Task	Command(s)
1.	Enable DHCP snooping globally on the switch.	**set dhcpsnooping enable**
2.	Determine where DHCP clients will be connected and enable DHCP snooping on their VLANs.	**set dhcpsnooping vlan** *vlan-list* **enable**
3.	Determine which ports will be connected to the DHCP server and configure them as trusted ports.	**set dhcpsnooping trust port** *port-string* **enable**
4.	If desired, enable logging of invalid DHCP messages on specfic ports.	**set dhcpsnooping log-invalid port** *port-string* **enable**
5.	If desired, add static bindings to the database.	**set dhcpsnooping binding** *mac-address* **vlan** *vlan-id ipaddr* **port** *port-string*

Configuration Notes

DHCP Server

- When the switch is operating in switch mode, then the DHCP server and DHCP clients must be in the same VLAN.
- If the switch is in routing mode (on those platforms that support routing), then the DCHP server can be remotely connected to a routing interface, or running locally.
- If the DHCP server is remotely connected, then the use of an IP helper address is required and MAC address verification should be disabled (**set dhcpsnooping verify mac-address disable**).
- The DHCP server must use Scopes in order to provide the IP addresses per VLAN.
- DHCP snooping must be enabled on the interfaces where the DHCP clients are connected, and the interfaces must be untrusted DHCP snooping ports.
- The routing interface that is connected to the DHCP server must be enabled for DHCP snooping and must be a trusted DHCP snooping port.

DHCP Snooping Commands

set dhcpsnooping

Use this command to enable or disable DHCP snooping globally.

Syntax

```
set dhcpsnooping {enable | disable}
```

Parameters

enable	Enable DHCP snooping globally on the switch.
disable	Disable DHCP snooping globally on the switch.

Defaults

Disabled globally.

Mode

Switch command, read-write.

Usage

By default, DHCP snooping is disabled globally and on all VLANs. You must enable it globally with this command, and then enable it on specific VLANs.

Example

The following example enables DHCP snooping globally.

```
C3(rw)->set dhcpsnooping enable
```

set dhcpsnooping vlan

Use this command to enable or disable DHCP snooping on a VLAN or range of VLANs.

Syntax

set dhcpsnooping vlan *vlan-range* {**enable** | **disable**}

Parameters

vlan-range	Specifies the VLAN or range of VLANs on which DHCP snooping is to be enabled or disabled.
enable | **disable**	Enables or disables DHCP snooping for the specified VLANs.

Defaults

DHCP snooping is disabled by default on all VLANs.

Mode

Switch command, read-write.

Usage

By default, DHCP snooping is disabled globally and on all VLANs. You must enable it globally with the **set dhcpsnooping** command, and then enable it on specific VLANs with this command.

Example

This example enables DHCP snooping on VLANS 10 through 20.

```
C3(rw)->set dhcpsnooping vlan 10-20 enable
```

set dhcpsnooping database write-delay

Use this command to specify the interval between updates to the stored bindings database.

Syntax

set dhcpsnooping database write-delay *seconds*

Parameters

second	Specify the interval in seconds between updates to the stored bindings database. The value can range from 15 to 86400 seconds.

Defaults

Every 5 minutes (300 seconds).

Mode

Switch command, read-write.

Usage

When a switch learns of new bindings or when it loses bindings, the switch updates the entries in the bindings database according to the write delay timer. The switch also updates the entries in the binding file. The frequency at which the file is updated is based on the delay configured with this command, and the updates are batched.

Example

The following example specifies that the stored database should be updated once an hour.

```
C3(rw)->set dhcpsnooping database write-delay 3600
```

set dhcpsnooping trust

Use this command to enable or disable a port as a DHCP snooping trusted port.

Syntax

set dhcpsnooping trust port *port-string* {**enable** | **disable**}

Parameters

port *port-string*	Specifies the port or ports to be enabled or disabled as trusted ports. The ports can be physical ports or LAGs that are members of a VLAN.
enable | **disable**	Enables or disables the specified ports as trusted ports.

Defaults

By default, ports are untrusted.

Mode

Switch command, read-write.

Usage

In order for DHCP snooping to operate, snooping has to be enabled globally and on specific VLANs, and the ports within the VLANs have to be configured as trusted or untrusted. On trusted ports, DHCP client messages are forwarded directly by the hardware. On untrusted ports, client messages are given to the DHCP snooping application.

The DHCP snooping application builds the bindings database from client messages received on untrusted ports. DHCP snooping creates a “tentative binding” from DHCP DISCOVER and REQUEST messages. Tentative bindings tie a client to the port on which the message packet was received. Tentative bindings are completed when DHCP snooping learns the client’s IP address from a DHCP ACK message on a trusted port.

The ports on the switch through which DHCP servers are reached must be configured as trusted ports so that packets received from those ports will be forwarded to clients. DCHP packets from a DHCP server (DHCP OFFER, DHCP ACK, DHCP NAK) are dropped if received on an untrusted port.

Example

This example configures port ge.1.1 as a trusted port.

```
C3(rw)->set dhcpsnooping trust port ge.1.1 enable
```

set dhcpsnooping binding

Use this command to add a static DHCP binding to the DHCP snooping database.

Syntax

set dhcpsnooping binding *mac-address* **vlan** *vlan-id ipaddr* **port** *port-string*

Parameters

mac-address	Specifies the MAC address of the binding entry.
vlan *vlan-id*	Specifies the VLAN of the binding entry.
ipaddr	Specifies the IP address of the binding entry.
port *port-string*	Specifies the port of the binding entry.

Defaults

None.

Mode

Switch command, read-write.

Usage

When enabled globally and on VLANs, DHCP snooping builds its bindings database from DHCP client messages received on untrusted ports. Such entries in the database are dynamic entries which will be removed in response to valid DECLINE, RELEASE, and NACK messages or when the absolute lease time of the entry expires.

You can add static entries to the bindings database with this command.

Example

This example creates a static entry, associating MAC address 00:01:02:33:44:55 with IP address 192.168.10.10 and VLAN 10, port ge.1.1.

```
C3(rw)->set dhcpsnooping binding 00:01:02:33:44:55 vlan 10 192.168.10.10 port
ge.1.1
```

set dhcpsnooping verify

Use this command to enable or disable DHCP snooping to filter on source MAC address.

Syntax

set dhcpsnooping verify mac-address {**enable** | **disable**}

Parameters

enable	Enables verification of the source MAC address in client messages against the client hardware address.
disable	Disables verification of the source MAC address in client messages against the client hardware address.

Defaults

Source MAC address verification is enabled by default.

Mode

Switch command, read-write.

Usage

When this verification is enabled, the DHCP snooping application compares the source MAC address contained in valid client messages with the client's hardware address. If there is a mismatch, DHCP snooping logs the event and drops the packet.

Use the **show dhcpsnooping** command to display the status (enabled or disabled) of source MAC address verification for each interface in an enabled VLAN. The **show dhcpsnooping statistics** command shows the actual number of MAC verification errors that occurred on untrusted ports.

Example

This example disables source MAC address verification and logging.

```
C3(rw)->set dhcpsnooping verify mac-address disable
```

set dhcpsnooping log-invalid

Use this command to enable or disable logging of invalid DHCP messages on ports.

Syntax

set dhcpsnooping log-invalid port *port-string* {**enable** | **disable**}

Parameters

port *port-string*	Specifies the port or ports on which to enable or disable logging of invalid packets.
enable | **disable**	Enables or disables logging on the specified ports.

Defaults

Disabled.

Mode

Switch command, read-write.

Usage

The DHCP snooping application processes incoming DHCP messages. For DHCPRELEASE and DHCPDECLINE messages, the application compares the receive interface and VLAN with the

client's interface and VLAN in the bindings database. If the interfaces do not match, the application logs the event if logging has been enabled.

Use the **show dhcpsnooping** command to display the status (enabled or disabled) of logging invalid packets for each interface in an enabled VLAN. The **show dhcpsnooping statistics** command shows the actual number of server messages received on untrusted ports.

Example

This example enables logging of invalid DHCP messages on port ge.1.1 and then displays the DHCP configuration settings.

```
C3(rw)->set dhcpsnooping log invalid port ge.1.1 enable
C3(su)->show dhcpsnooping
DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
3

 Interface    Trusted     Log Invalid Pkts
-----------  ----------   ----------------
ge.1.1       No           Yes
ge.1.2       No           No
ge.1.3       Yes          No
```

set dhcpsnooping limit

Use this command to configure rate limiting parameters for incoming DHCP packets on a port or ports.

Syntax

set dhcpsnooping limit *port-string* {**none** | **rate** *pps* {**burst interval** *secs*]}

Parameters

port-string	Specifies the port or ports to which to apply these rate limiting parameters.
none	Configures no limit on incoming DHCP packets.
rate *pps*	Specifies a rate limit in packets per second. The value of *pps* can range from 0 to 100 packets per second.
burst interval *secs*	Specifies a burst interval in seconds. The value of *secs* can range from 1 to 15 seconds.

Defaults

Rate = 15 packets per second

Burst Interval = 1 second

Mode

Switch command, read-write.

Usage

To protect the switch from DHCP attacks when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configured limit, DHCP snooping brings down the interface. You can re-enable the interface with the **set port enable** command. Both the rate and the burst interval can be configured.

You can display the currently configured rate limit parameters with the **show dhcpsnooping port** command.

Example

This example configures rate limit parameters on port ge.1.1.

```
C3(rw)->set dhcpsnooping limit ge.1.1 rate 20 burst interval 2
C3(rw)->show dhcpsnooping port ge.1.1
Interface     Trust State     Rate Limit      Burst Interval
                                 (pps)           (seconds)
----------   -------------   -------------   ---------------
    ge.1.1              No              20                 2
```

show dhcpsnooping

Use this command to display DHCP snooping configuration parameters.

Syntax

show dhcpsnooping

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command displays the status (enabled or disabled) of DHCP snooping globally, lists the VLANs on which DHCP snooping is enabled, displays whether source MAC address verification is enabled or disabled, and for ports that are enabled for snooping, displays whether they are trusted or untrusted and whether logging of invalid packets has been enabled.

Example

This example shows the output of the **show dhcpsnooping** command.

```
C3(su)->show dhcpsnooping
DHCP snooping is Enabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
```

```
3

 Interface    Trusted     Log Invalid Pkts
-----------  ----------   ----------------
ge.1.47      Yes          No
ge.1.48      No           No
lag.0.1      No           No
```

show dhcpsnooping database

Use this command to display DHCP snooping database configuration parameters.

Syntax

show dhcpsnooping database

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command displays where the database file is stored (locally) and what the write delay value is.

Example

This example shows the output of the **show dhcpsnooping database** command.

```
C3(su)->show dhcpsnooping database
agent url:  local

write-delay:  300
```

show dhcpsnooping port

Use this command to display DHCP snooping configuration parameters for specific ports.

Syntax

show dhcpsnooping port *port-string*

Parameters

port-string	Specifies the port or ports for which to display configuration information.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command displays the trust state and rate limiting parameters configured on the specified ports.

Example

This example shows the output of the **show dhcpsnooping port** command.

```
C3(su)->show dhcpsnooping port ge.1.1
Interface     Trust State     Rate Limit      Burst Interval
                                 (pps)           (seconds)
----------   -------------   -------------   ---------------
    ge.1.1              No              20                2
```

show dhcpsnooping binding

Use this command to display the contents of the DHCP snooping bindings database.

Syntax

show dhcpsnooping binding [**dynamic** | **static**] [**port** *port-string*] [**vlan** *vlan-id*]

Parameters

dynamic | **static**	(Optional) Limits the display of bindings in the database by type of entry, either dynamic or static.
port *port-string*	(Optional) Limits the display of bindings in the database by port.
vlan *vlan-id*	(Optional) Limits the display of bindings in the database by VLAN id.

Defaults

If no parameters are entered, all bindings in the database are displayed.

Mode

Switch command, read-write.

Usage

This command displays information about the DHCP bindings in the DHCP snooping database.

Example

This example shows the output of the **show dhcpsnooping binding** command when no parameters are entered.

```
C3(su)->show dhcpsnooping binding
Total number of bindings:  2
```

```
   MAC Address       IP Address     VLAN   Interface    Type    Lease (min)
-----------------  ---------------  ----  -----------  -------  -----------
00:02:B3:06:60:80    192.168.10.10     3       ge.1.1   STATIC
00:0F:FE:00:13:04    192.168.20.1      5      ge.1.30   DYNAMIC  1440
```

show dhcpsnooping statistics

Use this command to display DHCP snooping statistics for untrusted ports.

Syntax

show dhcpsnooping statistics

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Usage

The DHCP snooping application processes incoming DHCP messages on enabled untrusted interfaces. For DHCP RELEASE and DHCP DECLINE messages, the application compares the receive interface and VLAN with the client's interface and VLAN in the bindings database. If the interfaces do not match, the application logs the event (if logging of invalid messages is enabled) and drops the message. If source MAC verification is enabled, for valid client messages, DHCP snooping compares the source MAC address to the DHCP client hardware address. Where there is a mismatch, DHCP snooping logs and drops the packet.

This command displays, for each enabled untrusted interface, the number of source MAC verification failures and client interface mismatches that occurred since the last time these statistics were cleared.

Since DHCP servers should not be connected through an untrusted port, the DHCP snooping application will drop incoming DHCP server messages on untrusted interfaces and increment a counter that is displayed with this command.

Example

This example shows the output of the **show dhcpsnooping statistics** command.

```
C3(su)->show dhcpsnooping statistics
 Interface    MAC Verify   Client Ifc   DHCP Server
               Failures     Mismatch    Msgs Rec'd
-----------   ----------   ----------   -----------
ge.1.48               0            0             0
lag.0.1               0            0             0
```

clear dhcpsnooping binding

Use this command to remove bindings from the DHCP snooping bindings database.

Syntax

clear dhcpsnooping binding [**port** *port-string* | **mac** *mac-addr*]

Parameters

port *port-string*	(Optional) Specifies the entry or entries to remove by port identifier.
mac *mac-addr*	(Optional) Specifies the entry to remove by MAC address.

Defaults

If no parameters are entered, all bindings (static and dynamic) are removed.

Mode

Switch command, read-write.

Example

This example clears the static binding entry that includes port ge.1.2.

```
C3(su)->clear dhcpsnooping binding port ge.1.2
```

clear dhcpsnooping statistics

Use this command to clear the DHCP snooping statistics counters.

Syntax

clear dhcpsnooping statistics

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example clears the DHCP snooping statistics counters for all enabled untrusted ports.

```
C3(su)->clear dhcpsnooping statistics
```

clear dhcpsnooping database

Use this command to return the write delay value to its default value of 300 seconds.

Syntax

clear dhcpsnooping database [**write-delay**]

Parameters

write-delay	(Optional) Specifies that the write delay value should be returned to the default value of 300 seconds.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command will set the database write delay value to the default of 300 seconds.

Example

This example sets the database storage location to the default of local.

```
C3(su)->clear dhcpsnooping database
```

clear dhcpsnooping limit

Use this command to reset the rate limit values to the defaults of 15 packets per second with a burst interval of 1 second.

Syntax

clear dhcpsnooping limit *port-string*

Parameters

port-string	Specifies the port or ports to which this command applies.

Defaults

None.

Mode

Switch command, read-write.

Example

This example resets the rate limit values to their defaults on port ge.1.1.

```
C3(su)->clear dhcpsnooping limit ge.1.1
```

Dynamic ARP Inspection Overview

Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks where an unfriendly station

intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. ARP poisoning is a tactic where an attacker injects false ARP packets into the subnet, normally by broadcasting ARP responses in which the attacker claims to be someone else. By poisoning the ARP cache, a malicious user can intercept the traffic intended for other hosts on the network.

The Dynamic ARP Inspection application performs ARP packet validation. When DAI is enabled, it verifies that the sender MAC address and the source IP address are a valid pair in the DHCP snooping binding database and drops ARP packets whose sender MAC address and sender IP address do not match an entry in the database. Additional ARP packet validation can be configured.

If DHCP snooping is disabled on the ingress VLAN or the receive interface is trusted for DHCP snooping, ARP packets are dropped.

Functional Description

DAI is enabled on VLANs, effectively enabling DAI on the interfaces (physical ports or LAGs) that are members of that VLAN. Individual interfaces are configured as trusted or untrusted. The trust configuration for DAI is independent of the trust configuration for DHCP snooping. A trusted port is a port the network administrator does not consider to be a security threat. An untrusted port is one which could potentially be used to launch a network attack.

DAI considers all physical ports and LAGs untrusted by default.

Static Mappings

Static mappings are useful when hosts configure static IP addresses, DHCP snooping cannot be run, or other switches in the network do not run dynamic ARP inspection. A static mapping associates an IP address to a MAC address on a VLAN. DAI consults its static mappings before it consults DHCP snooping — thus, static mappings have precedence over DHCP snooping bindings.

ARP ACLs are used to define static mappings for DAI. In this implementation, only the subset of ARP ACL syntax required for DAI is supported. ARP ACLs are completely independent of ACLs used for QoS. A maximum of 100 ARP ACLs can be configured. Within an ACL, a maximum of 20 rules can be configured.

Optional ARP Packet Validation

If optional ARP packet validation has been configured, DAI verifies that the sender MAC address equals the source MAC address in the Ethernet header. Additionally, the option to verify that the target MAC address equals the destination MAC address in the Ethernet header can be configured. This check only applies to ARP responses, since the target MAC address is unspecified in ARP requests.

You can also enable IP address checking. When this option is enabled, DAI drops ARP packets with an invalid IP address. The following IP addresses are considered invalid:

- 0.0.0.0
- 255.255.255.255
- All IP multicast addresses
- All class E addresses (240.0.0.0/4)
- Loopback addresses (in the range 127.0.0.0/8)

Logging Invalid Packets

By default, DAI writes a log message to the normal buffered log for each invalid ARP packet it drops. You can configure DAI to not log invalid packets for specific VLANs.

Packet Forwarding

DAI forwards valid ARP packets whose destination MAC address is not local. The ingress VLAN could be a switching or routing VLAN. ARP requests are flooded in the VLAN. ARP responses are unicast toward their destination. DAI queries the MAC address table to determine the outgoing port. If the destination MAC address is local, DAI gives valid ARP packets to the ARP application.

Rate Limiting

To protect the switch from DHCP attacks when DAI is enabled, the DAI application enforces a rate limit for ARP packets received on untrusted interfaces. DAI monitors the receive rate on each interface separately. If the receive rate exceeds a configurable limit, DAI error disables the interface, which effectively brings down the interface. You can use the **set port enable** command to reenable the port.

You can configure both the rate and the burst interval. The default rate is 15 pps on each untrusted interface with a range of 0 to 100 pps. The default burst interval is 1 second with a range to 1 to 15 seconds.. The rate limit cannot be set on trusted interfaces since ARP packets received on trusted interfaces do not come to the CPU.

Eligible Interfaces

Dynamic ARP inspection is enabled per VLAN, effectively enabling DAI on the members of the VLAN, either physical ports or LAGs. Trust is specified on the VLAN members.

DAI cannot be enabled on port-based routing interfaces. It may be connected to:

- A single host through a trusted link (for example, a server)
- If multiple hosts need to connected, there must be a switch between the router and the hosts, with DAI enabled on that switch

Interaction with Other Functions

- DAI relies on the DHCP snooping application to verify that a {IP address, MAC address, VLAN, interface} tuple is valid.
- DAI registers with dot1q to receive notification of VLAN membership changes for the VLANs where DAI is enabled.
- DAI tells the driver about each untrusted interface (physical port or LAG) where DAI is enabled so that the hardware will intercept ARP packets and send them to the CPU.

Basic Configuration

The following basic configuration does not change the default rate limiting parameters.

Procedure 17-2 Basic Dynamic ARP Inspection Configuration

Step	Task	Command(s)
1.	Configure DHCP snooping.	Refer to Procedure 17-1 on page 17-3.
2.	Enable ARP inspection on the VLANs where clients are connected, and optionally, enable logging of invalid ARP packets.	**set arpinspection vlan** *vlan-range* [**logging**]
3.	Determine which ports are not security threats and configure them as DAI trusted ports.	**set arpinspection trust port** *port-string* **enable**
4.	If desired, configure optional validation parameters.	**set arpinspection validate** {[**src-mac**] [**dst-mac**] [**ip**]}
5.	If desired, configure static mappings for DAI by creating ARP ACLs: • Create the ARP ACL • Apply the ACL to a VLAN	**set arpinspection filter** *name* **permit ip host** *sender-ipaddr* **mac host** *sender-macaddr* **set arpinspection filter** *name* **vlan** *vlan-range* [**static**]

Example Configuration

Note: This example applies only to platforms that support routing.

The following example configures DHCP snooping and dynamic ARP inspection in a routing environment using RIP. The example configures two interfaces on the switch, configuring RIP on both interfaces, assigning each to a different VLAN, and then enabling DHCP snooping and dynamic ARP inspection on them:

- Interface ge.1.1, which is connected to a remote DHCP server, on VLAN 192
- Interface ge.1.2, which is connected to DHCP clients, on VLAN 10

In addition, the default VLAN, VLAN 1, is also enabled for DHCP snooping and dynamic ARP inspection.

Since the DHCP server is remote, the switch has been configured as a DHCP relay agent (with the **ip helper-address** command), to forward client requests to the DHCP server. Therefore, MAC address verification is disabled (with the **set dhcpsnooping verify mac-address disable** command) in order to allow DHCP RELEASE packets to be processed by the DHCP snooping functionality and client bindings removed from the bindings database

Router Configuration

```
router
enable
configure
interface vlan 10
no shutdown
ip address 10.2.0.1 255.255.0.0
ip helper-address 192.168.0.200
ip rip send version 2
ip rip receive version 2
ip rip enable
exit

interface vlan 192
no shutdown
ip address 192.168.0.1 255.255.255.0
ip rip send version 2
ip rip receive version 2
ip rip enable
exit
router rip
exit
```

VLAN Configuration

```
set vlan create 10
set vlan create 192
clear vlan egress 1 ge.1.1-2
```

```
set vlan egress 10 ge.1.2 untagged
set vlan egress 192 ge.1.1 untagged
```

DHCP Snooping Configuration

```
set dhcpsnooping enable
set dhcpsnooping vlan 1 enable
set dhcpsnooping vlan 10 enable
set dhcpsnooping vlan 192 enable
set dhcpsnooping verify mac-address disable
set dhcpsnooping trust port ge.1.1  enable
```

Dynamic ARP Inspection Configuration

```
set arpinspection vlan 1
set arpinspection vlan 10
set arpinspection vlan 192
set arpinspection trust port ge.1.1 enable
```

Dynamic ARP Inspection Commands

set arpinspection vlan

Use this command to enable dynamic ARP inspection on one or more VLANs, and optionally, enable logging of invalid ARP packets.

Syntax

set arpinspection vlan *vlan-range* [**logging**]

Parameters

vlan-range	Specifies the VLAN or range of VLANs on which to enable dynamic ARP inspection.
logging	(Optional) Enables logging of invalid ARP packets for that VLAN.

Defaults

Logging is disabled by default.

Mode

Switch command, read-write.

Usage

This command enables dynamic ARP inspection (DAI) on one or more VLANs. When DAI is enabled on a VLAN, DAI is effectively enabled on the interfaces (physical ports or LAGs) that are members of that VLAN.

DAI uses the DHCP snooping bindings database to verify that the sender MAC address and the source IP address are a valid pair in the database. ARP packets whose sender MAC address and sender IP address do not match an entry in the database are dropped.

If logging is enabled, invalid ARP packets are also logged.

Example

This example enables DAI on VLANs 2 through 5 and also enables logging of invalid ARP packets on those VLANs.

```
C3(su)->set arpinspection vlan 2-5 logging
```

set arpinspection trust

Use this command to enable or disable a port as a dynamic ARP inspection trusted port.

Syntax

set arpinspection trust port *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port or ports to be enabled or disabled as DAI trusted ports. The ports can be physical ports or LAGs that are members of a VLAN.
enable | **disable**	Enables or disables the specified ports as trusted for DAI.

Defaults

By default, all physical ports and LAGs are untrusted.

Mode

Switch command, read-write.

Usage

Individual interfaces are configured as trusted or untrusted. The trust configuration for DAI is independent of the trust configuration for DHCP snooping. A trusted port is a port the network administrator does not consider to be a security threat. An untrusted port is one which could potentially be used to launch a network attack.

DAI considers all physical ports and LAGs untrusted by default. Packets arriving on trusted interfaces bypass all DAI validation checks.

Example

This example enables port ge.1.1 as trusted for DAI.

```
C3(su)->set arpinspection trust port ge.1.1 enable
```

set arpinspection validate

Use this command to configure additional optional ARP validation parameters.

Syntax

`set arpinspection validate {[src-mac] [dst-mac] [ip]}`

Parameters

src-mac	Specifies that DAI should verify that the sender MAC address equals the source MAC address in the Ethernet header.
dst-mac	Specifies that DAI should verify that the target MAC address equals the destination MAC address in the Ethernet header. This check only applies to ARP responses, since the target MAC address is unspecified in ARP requests.
ip	Specifies that DAI should check the IP address and drop ARP packets with an invalid address. An invalid address is one of the following: • 0.0.0.0 • 255.255.255.255 • All IP multicast addresses • All class E addresses (240.0.0.0/4) • Loopback addresses (in the range 127.0.0.0/8)

Defaults

All parameters are optional, but at least one parameter must be specified.

Mode

Switch command, read-write.

Usage

This command adds additional validation of ARP packets by DAI, beyond the basic validation that the ARP packet's sender MAC address and sender IP address match an entry in the DHCP snooping bindings database.

Example

This example adds the optional verification that sender MAC addresses are the same as the source MAC addresses in the Ethernet headers of ARP packets.

```
C3(su)->set arpinspection validate src-mac
```

set arpinspection limit

Use this command to configure rate limiting parameters for incoming ARP packets on a port or ports

Syntax

set arpinspection limit port *port-string* {**none** | **rate** *pps* {**burst interval** *secs*]}

Parameters

port-string	Specifies the port or ports to which to apply these rate limiting parameters.
none	Configures no limit on incoming ARP packets.
rate *pps*	Specifies a rate limit in packets per second. The value of *pps* can range from 0 to 100 packets per second.
burst interval *secs*	Specifies a burst interval in seconds. The value of *secs* can range from 1 to 15 seconds.

Defaults

Rate = 15 packets per second

Burst Interval = 1 second

Mode

Switch command, read-write.

Usage

To protect the switch against DHCP attacks when DAI is enabled, the DAI application enforces a rate limit for ARP packets received on untrusted interfaces. DAI monitors the receive rate on each interface separately. If the receive rate exceeds the limit configured with this command, DAI disables the interface, which effectively brings down the interface. You can use the **set port enable** command to reenable the port.

You can configure both the rate and the burst interval. The default rate is 15 pps on each untrusted interface with a range of 0 to 100 pps. The default burst interval is 1 second with a range to 1 to 15 seconds.. The rate limit cannot be set on trusted interfaces since ARP packets received on trusted interfaces do not come to the CPU.

Example

This example sets the rate to 20 packets per second and the burst interval to 2 seconds on ports ge.1.1 and ge.1.2.

```
C3(su)->set arpinspection limit port ge.1.1-2 rate 20 burst interval 2
```

set arpinspection filter

Use this command to create an ARP ACL and then to assign an ACL to a VLAN, optionally as a static mapping.

Syntax

set arpinspection filter *name* {**permit ip host** *sender-ipaddr* **mac host** *sender-macaddr* | **vlan** *vlan-range* [**static**]}

Parameters

name	Specifies the name of the ARP ACL.
permit	Specifies that a permit rule is being created.
ip host *sender-ipaddr*	Specifies the IP address in the rule being created.
mac host *sender-macaddr*	Specifies the MAC address in the rule being created.
vlan *vlan-range*	Specifies the VLAN or VLANs to which this ARP ACL is assigned.
static	(Optional) Specifies that this ARP ACL configures static mappings for the VLAN or VLANs.

Defaults

None.

Mode

Switch command, read-write.

Usage

ARP ACLs are used to define static mappings for DAI. ARP ACLs are completely independent of ACLs used for QoS. A maximum of 100 ARP ACLs can be configured. Within an ACL, a maximum of 20 rules can be configured.

A static mapping associates an IP address to a MAC address on a VLAN. DAI consults its static mappings before it consults the DHCP snooping bindings database — thus, static mappings have precedence over DHCP snooping bindings.

Example

This example creates an ACL named staticARP and creates a permit rule for IP address 192.168.1.10. Then, the ACL is assigned to a VLAN as a static mapping.

```
C3(su)->set arpinspection filter staticARP permit ip host 192.168.1.10 mac host
00:01:22:33:44:55
C3(su)->set arpinspection filter staticARP vlan 10 static
```

show arpinspection access-list

Use this command to display ARP access list configuration information.

Syntax

show arpinspection access-list [*acl-name*]

Parameters

acl-name	(Optional) Specifies the ARP ACL to display.

Defaults

If a specific ACL is not specified, information about all configured ARP ACLs is displayed.

Mode

Switch command, read-write.

Example

This example displays information about the ARP ACL named staticARP.

```
C3(su)->show arpinspection access-list staticARP
ARP access list   staticARP
    permit ip host 192.168.1.10 mac host 00:01:22:33:44:55
    permit ip host 192.168.1.20 mac host 00:0A:11:22:33:66
```

show arpinspection ports

Use this command to display the ARP configuration of one or more ports.

Syntax

show arpinspection ports [*port-string*]

Parameters

port-string	(Optional) Specifies the port or ports for which to display ARP configuration information.

Defaults

If a port-string is not specified, information about all DAI-enabled untrusted ports is displayed.

Mode

Switch command, read-write.

Example

This example displays the ARP configuration of lag.0.1.

```
C3(su)->show arpinspection ports lag.0.1
Interface     Trust State     Rate Limit      Burst Interval
                                 (pps)          (seconds)
----------   -------------   -------------   ---------------
   lag.0.1              No              15                 1
```

show arpinspection vlan

Use this command to display the ARP configuration of one or more VLANs.

Syntax

show arpinspection vlan *vlan-range*

Parameters

vlan-range	Specifies the VLANs for which to display configuration information.

Defaults

None.

Mode

Switch command, read-write.

Example

This example displays ARP configuration information for VLAN 5.

```
C3(su)->show arpinspection vlan 5
Source MAC Validation                          Disabled
Destination MAC Validation                     Disabled
IP Address Validation                          Disabled

Vlan  Configuration Log Invalid           ACL Name                Static flag
----  ------------- ----------- -------------------------------  -----------
   5       Disabled     Enabled                         staticARP     Enabled
```

show arpinspection statistics

Use this command to display ARP statistics for all DAI-enabled VLANs or for specific VLANs.

Syntax

show arpinspection statistics [**vlan** *vlan-range*]

Parameters

vlan *vlan-range*	(Optional) Specifies the VLANs for which to display statistics.

Defaults

If no VLANs are specified, limited statistics for all DAI-enabled VLANs is displayed.

Mode

Switch command, read-write.

Usage

When no specific VLANs are entered, this command displays the number of Forwarded and Dropped ARP packets per DAI-enabled VLAN. When one or more VLANs are specified, this command displays more detailed statistics.

Examples

This example shows what is displayed when no VLANs are specified.

```
C3(su)->show arpinspection statistics
VLAN    Forwarded     Dropped
----   ------------  ---------
   5              0          0
```

This example shows what information is displayed when one or more VLANs are specified.

```
C3(su)->show arpinspection statistics vlan 5
VLAN    DHCP       ACL        DHCP       ACL       Bad Src   Bad Dest   Invalid
        Drops      Drops     Permits    Permits       MAC       MAC       IP
---- ---------- ---------- ---------- ---------- ---------- ---------- ---------
   5          0          0          0          0          0          0         0
```

clear arpinspection validate

Use this command to remove additional optional ARP validation parameters that were previously configured.

Syntax

clear arpinspection validate {[**src-mac**] [**dst-mac**] [**ip**]}

Parameters

src-mac	Clear, or remove, the verification that the sender MAC address equals the source MAC address in the Ethernet header.
dst-mac	Clear, or remove, the verification that the target MAC address equals the destination MAC address in the Ethernet header.
ip	Clear, or remove, checking the IP address and dropping ARP packets with an invalid address.

Defaults

All parameters are optional, but at least one parameter must be specified.

Mode

Switch command, read-write.

Usage

This command removes previously configured additional validation of ARP packets by DAI, beyond the basic validation that the ARP packet's sender MAC address and sender IP address match an entry in the DHCP snooping bindings database.

Use the **show arpinspection vlan** command to display the current status of the additional validation rules.

Example

This example removes all 3 additional validation conditions.

```
C3(su)->clear arpinspection validate src-mac dst-mac ip
```

clear arpinspection vlan

Use this command to disable dynamic ARP inspection on one or more VLANs or to disable logging of invalid ARP packets on one or more VLANs.

Syntax

clear arpinspection vlan *vlan-range* [**logging**]

Parameters

vlan-range	Specifies the VLAN or range of VLANs on which to disable dynamic ARP inspection.
logging	(Optional) Disable logging of invalid ARP packets for the specified VLANs.

Defaults

If logging is enabled for the specified VLAN but **logging** is not entered with this command, logging will remain enabled.

Mode

Switch command, read-write.

Usage

You can use this command to disable dynamic ARP inspection on one or more VLANs, or you can disable logging of invalid ARP packets on specified VLANs. To disable both logging and DAI, you must enter this command twice.

Example

This example first displays the DAI configuration for VLAN 5, then disables DAI on VLAN 5, then disables logging of invalid ARP packets on VLAN 5.

```
C3(su)->show arpinspection vlan 5

Source MAC Validation                          Disabled
Destination MAC Validation                     Disabled
IP Address Validation                          Disabled

Vlan  Configuration Log Invalid           ACL Name                Static flag
----  ------------- ----------- --------------------------------  -----------
   5        Enabled     Enabled                         staticARP     Enabled


C3(su)->clear arpinspection vlan 5


C3(su)->show arpinspection vlan 5

Source MAC Validation                          Disabled
Destination MAC Validation                     Disabled
IP Address Validation                          Disabled

Vlan  Configuration Log Invalid           ACL Name                Static flag
----  ------------- ----------- --------------------------------  -----------
   5       Disabled     Enabled                         staticARP     Enabled
```

```
C3(su)->clear arpinspection vlan 5 logging
C3(su)->show arpinspection vlan 5
Source MAC Validation                          Disabled
Destination MAC Validation                     Disabled
IP Address Validation                          Disabled

Vlan  Configuration Log Invalid           ACL Name                Static flag
----  ------------- ----------- -------------------------------  -----------
   5       Disabled    Disabled                         staticARP     Enabled
```

clear arpinspection filter

Use this command to remove an ARP ACL from a VLAN or from the switch, or to remove a permit rule from an existing ACL, or to change the status of static mapping to disabled.

Syntax

clear arpinspection filter *name* [**permit ip host** *sender-ipaddr* **mac host** *sender-macaddr*] | [**vlan** *vlan-range* [**static**]

Parameters

name	Specifies the name of the ARP ACL.
permit	(Optional) Specifies that a permit rule is being deleted.
ip host *sender-ipaddr*	Specifies the IP address in the rule being deleted.
mac host *sender-macaddr*	Specifies the MAC address in the rule being deleted.
vlan *vlan-range*	(Optional) Specifies the VLAN or VLANs to which this command should apply. Remove the ACL from the VLAN, if **static** is not specified also.
static	(Optional) Specifies that static mapping should be disabled for this ARP ACL for the specified VLAN or VLANs.

Defaults

If only the name is specified, the ACL is deleted from the switch.

Mode

Switch command, read-write.

Usage

You can use this command to:

- Remove a configured ARP ACL from the switch, or
- Remove a permit rule from a configured ARP ACL, or
- Remove the association of an ARP ACL with a VLAN or VLANs, or
- Disable static mapping of an ARP ACL associated with a VLAN or VLANs.

Use the **set arpinspection filter** command to create and assign an ARP ACL.

Use the **show arpinspection access-list** command to display currently configured ARP ACLs.

Examples

This example removes a permit rule from the ARP ACL named staticARP.

```
C3(su)->clear arpinspection filter staticARP permit ip host 192.168.1.10 mac host
00:01:22:33:44:55
```

This example disables static mapping of the ARP ACL named staticARP that is associated with VLAN 5.

```
C3(su)->clear arpinspection filter staticARP vlan 5 static
```

This example removes the ARP ACL named staticARP from VLAN 5.

```
C3(su)->clear arpinspection filter staticARP vlan 5
```

This example removes the ARP ACL named staticARP from the switch completely.

```
C3(su)->clear arpinspection filter staticARP
```

clear arpinspection limit

Use this command to return the DAI rate limiting values to their default values for a port or range of ports.

Syntax

clear arpinspection limit port *port-string*

Parameters

port-string	Specifies the ports on which to return the rate limiting values to defaults.

Defaults

Rate = 15 packets per second

Burst Interval = 1 second

Mode

Switch mode, read-write.

Usage

Use the **set arpinspection limit** command to change the values of the rate limit and burst interval.

Use the **show arpinspection ports** command to display the currently configured rate limits.

Example

This example returns the DAI rate limiting values to their defaults for port ge.1.1.

```
C3(su)->clear arpinspection limit port ge.1.1
```

clear arpinspection statistics

Use this command to clear all dynamic ARP inspection statistics.

Syntax

clear arpinspection statistics

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example clears all DAI statistics from the switch.

```
C3(su)->clear arpinspection statistics
```

18

Preparing for Router Mode

This chapter describes how to prepare the switch for routing.

Pre-Routing Configuration Tasks

Startup and general configuration of the SecureStack C3 switch must occur from the switch CLI. For details on how to start the switch and configure general platform settings, refer to Chapter 1, **Introduction**, Chapter 2, **Configuring Switches in a Stack**, and Chapter 3, **Basic Configuration**.

Once startup and general switch settings are complete, IP configuration and other router-specific commands can be executed when the switch is in router mode. For details on how to enable router mode from the switch CLI, refer to Table 18-2 in Enabling Router Configuration Modes.

The following pre-routing tasks must be performed from the switch CLI:

- Starting up the CLI. (“Using the Command Line Interface” on page 1-6)
- Setting the system password. (“set password” on page 3-5)
- Configuring basic platform settings, such as host name, system clock, and terminal display settings. (“Setting Basic Switch Properties” on page 3-9)
- Setting the system IP address. (“set ip address” on page 3-11)
- Creating and enabling VLANs. (Chapter 10)
- File management tasks, including uploading or downloading flash or text configuration files, and displaying directory and file contents. (“Managing Switch Configuration and Files” on page 3-39)
- Configuring the switch to run in router mode. (“Enabling Router Configuration Modes” on page 18-2)
- Enabling advanced router features. (“Activating Advanced Routing Features” on page 20-1)

Note: The command prompts used as examples in Table 18-1 and throughout this guide show switch operation for a user in admin (su) access mode, and a system where the VLAN 1 interface has been configured for routing. The prompt changes depending on your current configuration mode, your specific switch, and the interface types and numbers configured for routing on your system.

Table 18-1 Enabling the Switch for Routing

Step	To do this task...	Type this command...	At this prompt...	For details, see...
1	From admin (su) mode, enable router mode.	**router**	**Switch:** C3(su)->	
2	Enable router Privileged EXEC mode.	**enable**	**Router:** C3(su)->router>	
3	Enable global router configuration mode.	**configure**	**Router:** C3(su)->router#	
4	Enable interface configuration mode using the routing VLAN or loopback id.	**interface** {**vlan** *vlan-id* | **loopback** *loop-id*}	**Router:** C3(su)>router(Config)#	"interface" on page 19-3
5	Assign an IP address to the routing interface.	**ip address** {*ip-address ip-mask*}	**Router:** C3(su)->router (Config-if (Vlan 1))#	"interface" on page 19-3
6	Enable the interface for IP routing.	**no shutdown**	**Router:** C3(su)->router(Config-if (Vlan 1))#	"no shutdown" on page 19-6

Example

The following example shows how to configure VLAN 1 on IP address 182.127.63.1 255.255.255.0 as a routing interface.

```
C3(su)->router
C3(su)->router>enable
C3(su)->router#configure
 Enter configuration commands:
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip address 182.127.63.1 255.255.255.0
C3(su)->router(Config-if(Vlan 1))#no shutdown
```

Enabling Router Configuration Modes

The SecureStack C3 CLI provides different modes of router operation for issuing a subset of commands from each mode. Table 18-2 describes these modes of operation.

Table 18-2 Router CLI Configuration Modes

Use this mode...	To...	Access method...	Resulting Prompt...
Privileged EXEC Mode	Set system operating parameters Show configuration parameters Save/copy configurations	From the switch CLI: Type **router**, then Type **enable**.	 C3(su)->router> C3(su)->router#
Global Configuration Mode	Set system-wide parameters.	Type **configure** from Privileged EXEC mode.	C3(su)->router (Config)#
Interface Configuration Mode	Configure router interfaces.	Type **interface vlan** or **loopback** and the interface's id from Global Configuration mode.	C3(su)->router(Config-if (Vlan 1))# C3(su)->router(Config-if (Lpbk 1))#

Table 18-2 Router CLI Configuration Modes (Continued)

Use this mode...	To...	Access method...	Resulting Prompt...
Router Configuration Mode	Set IP protocol parameters.	Type **router** and the protocol *name* (and, for OSPF, the instance ID**)** from Global or Interface Configuration mode.	C3(su)->router(Config-router)#

Note: To jump to a lower configuration mode, type **exit** at the command prompt. To revert back to switch CLI, type exit from Privileged EXEC router mode.

19

IP Configuration

This chapter describes the Internet Protocol (IP) configuration set of commands and how to use them.

Router: Unless otherwise noted, the commands covered in this chapter can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to “Enabling Router Configuration Modes” on page 18-2.

Configuring Routing Interface Settings

Purpose

To enable routing interface configuration mode on the device, to create routing interfaces, to review the usability status of interfaces configured for IP, to set IP addresses for interfaces, to enable interfaces for IP routing at device startup, and to review the running configuration.

Note: For information about configuring tunnel interfaces, see “Configuring Tunnel Interfaces” on page 19-8.

Commands

For information about...	Refer to page...
show running-config	19-6
no shutdown	19-6
no ip routing	19-7

show interface

Use this command to display information about one or more interfaces (VLANs or loopbacks) configured on the router.

Syntax

show interface [**vlan** *vlan-id*] [**loopback** *loop-id*]

Parameters

vlan *vlan*-id	(Optional) Displays interface information for a specific VLAN interface. This interface must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.
loopback *loop-id*	(Optional) Displays interface information for a specific loopback interface.

Defaults

If interface type is not specified, information for all routing interfaces will be displayed.

Mode

Any router mode.

Examples

This example shows how to display information for all interfaces configured on the router. For a detailed description of this output, refer to Table 19-1:

```
C3(su)->router#show interface
Vlan 1 is Administratively DOWN
 Vlan 1 is Operationally DOWN
 Mac Address is: 0001.f4da.2cba
 The name of this device is Vlan 1
 The MTU is 1500 bytes
 The bandwidth is 10000 Mb/s
 Encapsulation ARPA, Loopback not set
 ARP type: ARPA, ARP Timeout: 14400 seconds
```

This example shows how to display information for loopback interface 1.

```
C3(su)->router#show interface loopback 1

Loopback 1 is Administratively UP
Loopback 1 is Operationally UP
Internet Address is 10.1.192.100, Subnet Mask is 255.255.255.0
The name of this device is Loopback 1
The MTU is 1500 bytes
```

interface

Use this command to configure interfaces for IP routing.

Syntax

interface vlan *vlan-id* | **loopback** *loop-id*

Parameters

vlan *vlan*-id	Specifies the number of the VLAN interface to be configured for routing. This interface must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.
loopback *loop-id*	Specifies the number of the loopback interface to be configured for routing. The value of *loop-id* can range from 0 to 7.

Defaults

None.

Mode

Router global configuration mode: C3(su)->router(Config)#

Usage

This command enables interface configuration mode from global configuration mode, and, if the interface has not previously been created, this command creates a new routing interface. For details on configuration modes supported by the SecureStack C3 device and their uses, refer to Table 18-2 in "Enabling Router Configuration Modes" on page 18-2.

VLANs must be created from the switch CLI before they can be configured for IP routing. For details on creating VLANs and configuring them for IP, refer to "Enabling Router Configuration Modes" on page 18-2.

Each VLAN interface must be configured for routing separately using the **interface** command. To end configuration on one interface before configuring another, type **exit** at the command prompt. Enabling interface configuration mode is required for completing interface-specific configuration tasks. For an example of how these commands are used, refer to "Pre-Routing Configuration Tasks" on page 18-1.

A loopback interface is always expected to be up. This interface can provide the source address for sent packets and can receive both local and remote packets. The loopback interface is typically used by routing protocols, but it can also be used for management or network services such as RADIUS, SNMP, Syslog, SNTP, or sFlow. By default, if RADIUS is configured with no host IP address on the device, it will use the loopback interface 0 IP address (if it has been configured) as its source for the NAS-IP attribute. (Administrators can assign where to source management or network service IP packets via the **set interfac**e commands.)

Each SecureStack C3 system (stack) can support up to 24 routing interfaces. Each interface can be configured for the RIP and/or OSPF routing protocols.

Note: For information about configuring tunnel interfaces, see "Configuring Tunnel Interfaces" on page 19-8.

Examples

This example shows how to enter configuration mode for VLAN 1:

```
C3(su)->router#configure
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#
```

This example shows how to enter configuration mode for loopback 1:

```
C3(su)->router#configure
C3(su)->router(Config)#interface loopback 1
C3(su)->router(Config-if(Lpbk 1))#
```

show ip interface

Use this command to display information, including administrative status, IP address, MTU (Maximum Transmission Unit) size and bandwidth, and ACL configurations, for interfaces configured for IP.

Syntax

show ip interface [**vlan** *vlan-id*] [**loopback** *loop-id*]

Parameters

vlan *vlan*-id	(Optional) Displays information for a specific VLAN interface. This interface must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.
loopback *loop-id*	(Optional) Displays interface information for a specific loopback interface.

Defaults

If interface type is not specified, status information for all routing interfaces will be displayed.

Mode

Any router mode.

Example

This example shows how to display configuration information for VLAN 1:

```
C3(su)->router#show ip interface vlan 1

Vlan 1 is Admin DOWN
Vlan 1 is Oper DOWN
Primary IP Address is 192.168.10.1    Mask 255.255.255.0
Frame Type Ethernet
MAC-Address 0001.F45C.C993
Incoming Accesslist is not set
Outgoing AccessList is not set
MTU is 6145 bytes
ARP Timeout is 1 seconds
Direct Broadcast Disabled
Proxy ARP is Disabled
```

Table 19-1 provides an explanation of the command output.

Table 19-1 show ip interface Output Details

Output Field	What It Displays...
Vlan *N*	Whether the interface is administratively and operationally up or down.
Primary IP Address	Inteface's primary IP address and mask. Set using the **ip address** command as described in "ip address" on page 19-5.
Frame Type	Encapsulation type used by this interface. Set using the **arp** command as described in "arp" on page 19-13.
MAC-Address	MAC address mapped to this interface.
Incoming Access List	Whether or not an access control list (ACL) has been configured for ingress on this interface using the commands described in "Configuring Access Lists" on page 26-79.
Outgoing Access List	Not supported.
MTU	Interface's Maximum Transmission Unit size.
ARP Timeout	Duration for entries to stay in the ARP table before expiring. Set using the **arp timeout** command as described in "arp timeout" on page 19-15.
Direct Broadcast	Whether or not IP directed broadcast is enabled. Set using the ip directed-broadcast command described in "ip directed-broadcast" on page 19-16.
Proxy Arp	Whether or not proxy ARP is enabled or disabled for this interface. Set using the **ip proxy arp** command as described in "ip proxy-arp" on page 19-14.

ip address

Use this command to set, remove, or disable a primary or secondary IP address for an interface. The **no** form of this command removes the specified IP address and disables the interface for IP processing.

Syntax

```
ip address ip-address ip-mask [secondary]
no ip address ip-address ip-mask
```

Parameters

ip-address	Specifies the IP address of the interface to be added or removed.
ip-mask	Specifies the mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured IP address is a secondary address.

Defaults

If **secondary** is not specified, the configured address will be the primary address for the interface.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

Each SecureStack C3 system supports up to 24 routing interfaces, with up to 8 secondary addresses allowed for each primary IP address.

Example

This example sets the IP address to 192.168.1.1 and the network mask to 255.255.255.0 for VLAN 1:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip address 192.168.1.1 255.255.255.0
```

show running-config

Use this command to display the non-default, user-supplied commands entered while configuring the device.

Syntax

`show running-config`

Parameters

None.

Defaults

None.

Mode

Any router mode.

Example

This example shows how to display the current router operating configuration:

```
C3(su)->router#show running-config
!
interface vlan 10
  ip address 99.99.2.10 255.255.255.0
  no shutdown
!
 router ospf 1
  network 99.99.2.0     0.0.0.255 area 0.0.0.0
network 192.168.100.1 0.0.0.0   area 0.0.0.0
```

no shutdown

Use this command to enable an interface for IP routing and to allow the interface to automatically be enabled at device startup.

Syntax

`no shutdown`

`shutdown`

Parameters

None.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

The shutdown form of this command disables an interface for IP routing.

Example

This example shows how to enable VLAN 1 for IP routing:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#no shutdown
```

no ip routing

Use this command to disable IP routing on the device. By default, IP routing is enabled when interfaces are configured for it as described in "Configuring Routing Interface Settings" on page 19-1.

Syntax

```
no ip routing
```

Parameters

None.

Mode

Global configuration: C3(su)->router(Config)#

Defaults

None.

Example

This example shows how to disable IP routing on the device:

```
C3(su)->router(Config)#no ip routing
```

Configuring Tunnel Interfaces

Purpose

The commands in this section describe how to create, delete, and manage tunnel interfaces. Several different types of tunnels provide functionality to facilitate the transition of IPv4 networks to IPv6 networks. These tunnels are divided into two classes: configured and automatic. The distinction is that configured tunnels are explicitly configured with a destination or endpoint of the tunnel. Automatic tunnels, in contrast, infer the endpoint of the tunnel from the destination address of packets routed into the tunnel.

For information about configuring IPv6 parameters on tunnel interfaces, such as an IPv6 address, see Chapter 22, **IPv6 Configuration**.

Note: IPv6 routing must be enabled with an IPv6 routing license key in order for these commands to be visible in the CLI.

Commands

For information about...	Refer to page...
interface tunnel	19-8
tunnel source	19-9
tunnel destination	19-10
tunnel mode	19-10
show interface tunnel	19-11

interface tunnel

Use this command to configure a tunnel interface.

Syntax

```
interface tunnel tunnel-id
no interface tunnel tunnel-id
```

Parameters

tunnel-id	Specifies the number of the tunnel interface to be configured for routing. The value of *tunnel-id* can range from 0 to 7.

Defaults

None.

Mode

Router global configuration mode: C3(su)->router(Config)#

Usage

This command enables tunnel interface configuration mode from global configuration mode, and, if the interface has not previously been created, this command creates a new tunnel routing interface.

The **no** form of this command removes the tunnel interface and associated configuration parameters.

Example

This example creates a configured tunnel interface 1.

```
C3(su)->router(Config)# interface tunnel 1
C3(su)->router(Config-if(Tnnl 1))#
```

tunnel source

This command specifies the IPv4 source transport address of the tunnel.

Syntax

```
tunnel source {ipv4-addr | interface vlan vlan-id}
no tunnel source
```

Parameters

ipv4-addr	The IPv4 source address of the tunnel.
interface vlan *vlan-id*	Specify an interface to use a link-local address. The VLAN must be configured in switch mode.

Defaults

None.

Mode

Router interface configuration: C3**(su)->router(Config-if(Tnnl 1))#**

Usage

The **no** form of this command removes the source IPv4 address for the tunnel interface being configured.

Example

The following example configures the source IPv4 address for tunnel 1.

```
C3(su)->router(Config)# interface tunnel 1
C3(su)->router(Config-if(Tnnl 1))#
C3(su)->router(Config-if(Tnnl 1))# tunnel source 192.168.10.10
```

tunnel destination

This command specifies the IPv4 destination transport address of the tunnel.

Syntax

tunnel destination *ipv4-addr*
no tunnel destination

Parameters

ipv4-addr	The IPv4 destination address of the tunnel.

Defaults

None.

Mode

Router interface configuration: C3**(su)->router(Config-if(Tnnl 1))#**

Usage

The **no** form of this command removes the destination IPv4 address for the tunnel interface being configured.

Example

The following example configures the destination IPv4 address for tunnel 1.

```
C3(su)->router(Config)# interface tunnel 1
C3(su)->router(Config-if(Tnnl 1))#
C3(su)->router(Config-if(Tnnl 1))# tunnel destination 192.168.10.20
```

tunnel mode

This command specifies the mode of the tunnel interface.

Syntax

tunnel mode ipv6ip
no tunnel mode ipv6ip

Parameters

ipv6ip	Specifies that the tunnel mode is IPv6 over IPv4

Defaults

None.

Mode

Router interface configuration: C3**(su)->router(Config-if(Tnnl 1))#**

Usage

The **no** form of this command removes the mode of the tunnel.

Example

This example sets the tunnel mode to IPv6 over IPv4.

```
C3(su)->router(Config)# interface tunnel 1
C3(su)->router(Config-if(Tnnl 1))#
C3(su)->router(Config-if(Tnnl 1))# tunnel mode ipv6ip
```

show interface tunnel

This command displays information about a configured tunnel interface.

Syntax

show interface tunnel *tunnel-id*

Parameters

tunnel-id	Specifies the tunnel for which to display information.

Defaults

None.

Mode

Router global configuration: C3(su)->router(Config)#

Router privileged exec: C3(su)->router#

Usage

Use this command to display general interface information. Refer to in Chapter 22, **IPv6 Configuration** for a description of the **show ipv6 interface tunnel** command.

Example

This example shows the output of this command.

```
C3(su)->router(Config)#show interface tunnel 1

Tunnel 1 is Operationally DOWN
The name of this device is Tunnel 1
The MTU is 1480 bytes
```

Reviewing and Configuring the ARP Table

Purpose

To review and configure the routing ARP table, to enable proxy ARP on an interface, and to set a MAC address on an interface.

Commands

show ip arp

Use this command to display entries in the ARP (Address Resolution Protocol) table. ARP converts an IP address into a physical address.

Syntax

show ip arp [*ip-address*]|[**vlan** *vlan-id*]|[*output-modifier*]

Parameters

ip-address	(Optional) Displays ARP entries related to a specific IP address.
vlan *vlan-id*	(Optional) Displays only ARP entries learned through a specific VLAN interface. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.
output-modifier	(Optional) Displays ARP entries within a specific range. Options are: – | **begin** *ip-address* — Displays only ARP entries that begin with the specified IP address. – | **exclude** *ip-address* — Excludes ARP entries matching the specified IP address. – | **include** *ip-address* — Includes ARP entries matching the specified IP address.

Defaults

If no parameters are specified, all entries in the ARP cache will be displayed.

Mode

Any router mode.

Example

This example shows how to use the **show ip arp** command:

```
C3(su)->router#show ip arp
Protocol     Address          Age (min) Hardware Addr   Type      Interface
--------------------------------------------------------------------------------
Internet     134.141.235.251     0      0003.4712.7a99  ARPA      Vlan1
Internet     134.141.235.165     -      0002.1664.a5b3  ARPA     Vlan1
Internet     134.141.235.167     4      00d0.cf00.4b74  ARPA     Vlan2

C3(su)->router#show ip arp 134.141.235.165
Protocol     Address          Age (min)  Hardware Addr Type       Interface
--------------------------------------------------------------------------------
Internet     134.141.235.165     -      0002.1664.a5b3  ARPA      Vlan2

C3(su)->router#show ip arp vlan 2
Protocol     Address          Age (min) Hardware Addr Type        Interface
--------------------------------------------------------------------------------
Internet     134.141.235.251     0      0003.4712.7a99 ARPA       Vlan2
```

Table 19-2 provides an explanation of the command output.

Table 19-2 show ip arp Output Details

Output Field	What It Displays...
Protocol	ARP entry's type of network address.
Address	Network address mapped to the entry's MAC address.
Age (min)	Interval (in minutes) since the entry was entered in the table.
Hardware Addr	MAC address mapped to the entry's network address.
Type	Encapsulation type used for the entry's network address.
Interface	Interface (VLAN or loopback) through which the entry was learned.

arp

Use this command to add or remove permanent (static) ARP table entries. Up to 1,000 static ARP entries are supported per SecureStack C3 system. A multicast MAC address can be used in a static ARP entry. The **no** form of this command removes the specified permanent ARP entry:

Syntax

```
arp ip-address mac-address
no arp ip-address
```

Parameters

ip-address	Specifies the IP address of a device on the network. Valid values are IP addresses in dotted decimal notation.
mac-address	Specifies the 48-bit hardware address corresponding to the *ip-address* expressed in hexadecimal notation.

Defaults

None.

Mode

Global configuration: C3**(su)->router(Config)#**

Usage

The IP address specified for the static ARP entry must fall within one of the subnets or networks defined on the routed interfaces of the system (or stack, if applicable). The system can then match the IP address of the static ARP entry with the appropriate routed interface and associate it with the correct VLAN.

Example

This example shows how to add a permanent ARP entry for the IP address 130.2.3.1 and MAC address 0003.4712.7a99:

```
C3(su)->router(Config)#arp 130.2.3.1 0003.4712.7a99
```

ip proxy-arp

Use this command to enable proxy ARP on an interface. The **no** form of this command disables proxy ARP.

Syntax

ip proxy-arp

no ip proxy-arp

Parameters

None.

Defaults

Disabled.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

This variation of the ARP protocol allows the router to send an ARP response on behalf of an end node to the requesting host. Proxy ARP can be used to resolve routing issues on end stations that are unable to route in the subnetted environment. The SecureStack C3 will answer to ARP requests on behalf of targeted end stations on neighboring networks. It is disabled by default.

Example

This example shows how to enable proxy ARP on VLAN 1:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip proxy-arp
```

arp timeout

Use this command to set the duration (in seconds) for dynamically learned entries to remain in the ARP table before expiring. The **no** form of this command restores the default value of 14,400 seconds.

arp timeout *seconds*
no arp timeout

Parameters

seconds	Specifies the time in seconds that an entry remains in the ARP cache. Valid values are **0** - **65535**. A value of 0 specifies that ARP entries will never be aged out.

Defaults

14,400 seconds.

Mode

Global configuration: C3(su)->router(Config)#

Example

This example shows how to set the ARP timeout to 7200 seconds:

```
C3(su)->router(Config)#arp timeout 7200
```

clear arp-cache

Use this command to delete all nonstatic (dynamic) entries from the ARP table.

clear arp-cache

Parameters

None.

Mode

Privileged EXEC: C3**(su)->router#**

Defaults

None.

Example

This example shows how to delete all dynamic entries from the ARP table:

```
C3(su)->router#clear arp-cache
```

Configuring Broadcast Settings

Purpose

To configure IP broadcast settings. By default, interfaces on the SecureStack C3 do not forward broadcast packets.

Commands

ip directed-broadcast

Use this command to enable or disable IP directed broadcasts on an interface. By default, interfaces on the SecureStack C3 do not forward directed broadcasts. The **no** form of this command disables IP directed broadcast on the interface.

Syntax

```
ip directed-broadcast
no ip directed-broadcast
```

Parameters

None.

Defaults

None.

Mode

Interface configuration: C3(su)->Router1(Config-if(Vlan 1))#

Usage

Directed broadcast is an efficient mechanism for communicating with multiple hosts on a network while only transmitting a single datagram. A directed broadcast is a packet sent to all hosts on a specific network or subnet. The directed broadcast address includes the network or subnet fields, with the binary bits of the host portion of the address set to one. For example, for a network with the address 192.168.0.0/16, the directed broadcast address would be 192.168.255.255. For a subnet with the address 192.168.12.0/24, the directed broadcast address would be 192.168.12.255.

In order to minimize broadcast DoS attacks, forwarding of directed broadcasts is disabled by default on the SecureStack C3, as recommended by RFC 2644.

If the ability to send directed broadcasts to a network is required, you should enable directed broadcasts only on the one interface that will be transmitting the datagrams. For example, if a SecureStack C3 has five routed interfaces for the 10, 20, 30, 40, and 50 networks, enabling directed

broadcast only on the 30 network interface will allow anyone from any other networks (10, 20, 40, 50) to send directed broadcast to the 30 network.

Example

This example shows how to enable IP directed broadcasts on VLAN 1:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip directed-broadcast
```

ip forward-protocol

Use this command to enable UDP broadcast forwarding and specify which protocols will be forwarded.

Syntax

ip forward-protocol udp [*port*]

no ip forward-protocol udp [*port*]

Parameters

udp	Specifies UDP as the IP forwarding protocol.
port	(Optional) Specifies a destination port that controls which UDP services are forwarded.

Defaults

If *port* is not specified, the following defaults are used:

- Trivial File Transfer Protocol (TFTP) (port 69)
- Domain Naming System (port 53)
- Time service (port 37)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS service (port 49)
- EN-116 Name Service (port 42)

Mode

Router command, Global configuration: C3(su)->router(Config)#

Router interface configuration: C3(su)->router(Config-if(Vlan 1)#

Usage

In order to actually forward protocols, you must configure an IP helper address on the individual router interfaces with the command "ip helper-address" (page 19-18).

If a certain service exists inside the node, and there is no need to forward the request to remote networks, the "no" form of this command should be used to disable the forwarding for the specific port. Such requests will not be automatically blocked from being forwarded just because a service for them exists in the node.

The **no** form of this command removes a UDP port or protocol, disabling forwarding.

Examples

The following example globally disables IP forwarding for UDP port 69.

```
C3(su)->router(Config)#no ip forward-protocol udp 69
```

The following example disables IP forwarding for UDP port 69 on a specific interface.

```
C3(su)->router(Config)#interface vlan 10
C3(su)->router(Config-if(Vlan 10))#no ip forward-protocol udp 69
```

ip helper-address

Use this command to enable the DHCP/BOOTP relay agent on a SecureStack C3 routed interface and/or to forward broadcast traffic identified with the ip forward-protocol command to a unicast address. Enabling the relay agent allows forwarding of client DHCP/BOOTP requests to a DHCP/BOOTP server that does not reside on the same broadcast domain as the client. Up to 6 IP helper addresses may be configured per interface.

The **no** form of this command disables the forwarding of UDP datagrams to the specified address.

Syntax

ip helper-address *address*
no ip helper-address *address*

Parameters

address	Address of the host where UDP broadcast packets should be forwarded.

Defaults

None.

Mode

Interface configuration: C3(su)->Router1(Config-if(Vlan 1))#

Usage

Typically for DHCP/BootP, when a host requests an IP address, it sends out a DHCP broadcast packet. Normally, the router drops all broadcast packets. However, by executing this command, you enable the routed interface to pass DHCP broadcast frames through, sending them directly to the remote DHCP server's IP address.

The DHCP/BOOTP relay agent will detect DHCP/BOOTP requests based on UDP source and destination ports. It will then make the necessary changes to the packet and send the packet to the DHCP server. The changes include:

- Replacing the destination IP address with the address of the DHCP server,
- Replacing the source IP address with its own address (that is, the IP address of the local routed interface), and
- Within the BOOTP part of the packet, changing the Relay Agent IP address from 0.0.0.0 to the address of the local routed interface.

The last change to the BootP packet "tells" the DHCP server that it needs to assign an IP address that is in the same subnet as the Relay Agent IP. When the response comes from the server, the DHCP/BOOTP relay agent sends it to the host.

For other protocols specified through the ip forward-protocol command, the system forwards broadcast UDP traffic as a unicast packet to the specified IP addresses.

Example

This example show how to have all client DHCP requests for users in VLAN 1 to be forwarded to the remote DHCP server with IP address 192.168.1.28.

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip helper-address 192.168.1.28
```

Reviewing IP Traffic and Configuring Routes

Purpose

To review IP traffic and configure routes, to send router ICMP (ping) messages, and to execute traceroute.

Commands

For information about...	Refer to page...
show ip route	19-19
ip route	19-21
ping	19-21
traceroute	19-22

show ip route

Use this command to display information about IP routes.

Syntax

show ip route [*destination-prefix* [*destination-prefix-match*] | **connected** | **ospf** | **rip** | **static** | **summary**]

Parameters

destination-prefix *destination-prefix-match*	(Optional) Converts the specified address and mask into a prefix and displays any routes that match the prefix.
connected	(Optional) Displays connected routes.
ospf	(Optional) Displays routes configured for the OSPF routing protocol. For details on configuring OSPF, refer to "Configuring OSPF" on page 20-11.
rip	(Optional) Displays routes configured for the RIP routing protocol. For details on configuring RIP, refer to "Configuring RIP" on page 20-2.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of the IP routing table.

Defaults

If no parameters are specified, all IP route information will be displayed.

Mode

Any router mode.

Usage

The routing table contains all active static routes, all the RIP routes, and up to three best OSPF routes learned for each network.

Example

This example shows how to use the **show ip route** command to display all IP route information. A portion of the output is shown:

```
C3(su)->router#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, IA - OSPF interarea
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       E - EGP, i - IS-IS, L1 - IS-IS level-1, LS - IS-IS level-2
       * - candidate default, U - per user static route

IA   1.255.255.248/29 [10/30] via 168.0.0.249, Vlan 3205
O    2.0.0.0/10 [8/30] via 168.1.0.254, Vlan 1200
O    2.224.0.0/11 [8/30] via 168.1.0.254, Vlan 1200
C    7.15.0.0/24 [0/0] directly connected, Vlan 715
O    11.11.12.12/32 [8/30] via 168.0.0.249, Vlan 3205
O    11.11.13.13/32 [8/10] via 168.1.0.249, Vlan 1300
O    11.11.16.16/32 [8/20] via 168.0.0.249, Vlan 3205
E2   11.11.17.17/32 [150/20] via 168.0.0.249, Vlan 3205
IA   11.11.21.21/32 [10/30] via 168.0.0.249, Vlan 3205
IA   11.11.22.22/32 [10/30] via 168.0.0.249, Vlan 3205
E2   11.11.24.24/32 [150/20] via 168.0.0.249, Vlan 3205
O    11.11.25.25/32 [8/20] via 168.0.0.249, Vlan 3205
C    11.11.26.26/32 [0/0] directly connected, Loopback 0
O    11.11.27.27/32 [8/10] via 168.1.0.254, Vlan 1200
O    11.11.28.28/32 [8/20] via 168.1.0.254, Vlan 1200
E2   12.0.0.0/17 [150/20] via 168.0.0.249, Vlan 3205
E2   19.0.0.0/30 [150/20] via 168.0.0.249, Vlan 3205
IA   20.0.0.0/24 [10/40] via 168.0.0.249, Vlan 3205
E2   22.22.0.0/16 [150/20] via 168.0.0.249, Vlan 3205
E2   22.22.10.0/24 [150/20] via 168.0.0.249, Vlan 3205
E2   22.22.12.0/24 [150/20] via 168.0.0.249, Vlan 3205
O    22.22.13.0/24 [8/30] via 168.1.0.254, Vlan 1200
E2   22.22.14.0/24 [150/20] via 168.0.0.249, Vlan 3205
O    22.22.15.0/24 [8/20] via 168.1.0.249, Vlan 1300 via 168.1.0.254, Vlan 1200
E2   22.22.16.0/24 [150/20] via 168.0.0.249, Vlan 3205
E2   22.22.17.0/24 [150/20] via 168.0.0.249, Vlan 3205
O    22.22.18.0/24 [8/30] via 168.1.0.254, Vlan 1200
O    22.22.19.0/24 [8/20] via 168.1.0.249, Vlan 1300 via 168.1.0.254, Vlan 1200
IA   22.22.20.0/24 [10/40] via 168.0.0.249, Vlan 3205
IA   22.22.21.0/24 [10/50] via 168.0.0.249, Vlan 3205
IA   22.22.22.0/24 [10/30] via 168.0.0.249, Vlan 3205
O    22.22.23.0/24 [8/30] via 168.0.0.249, Vlan 3205
IA   22.22.24.0/24 [10/40] via 168.0.0.249, Vlan 3205
E2   22.22.25.0/24 [150/20] via 168.0.0.249, Vlan 3205
E2   22.22.26.0/24 [150/20] via 168.0.0.249, Vlan 3205
C    22.22.27.0/24 [0/0] directly connected, Vlan 4027
```

```
O    22.22.28.0/24 [8/20] via 168.1.0.249, Vlan 1300 via 168.1.0.254, Vlan 1200
E2   22.22.29.0/24 [150/20] via 168.0.0.249, Vlan 3205
C    26.0.0.0/8 [0/0] directly connected, Vlan 26
O    33.9.8.0/28 [8/20] via 168.1.0.254, Vlan 1200
E2   33.33.0.0/16 [150/20] via 168.0.0.249, Vlan 3205
```

ip route

Use this command to add or remove a static IP route. The **no** form of this command removes the static IP route.

ip route *prefix mask dest-addr* [*distance*]
no ip route *prefix mask forward-addr*

Parameters

prefix	Specifies a destination IP address prefix.
mask	Specifies a destination prefix mask.
dest-addr	Specifies a forwarding (gateway) IP address.
distance	(Optional) Specifies an administrative distance metric for this route. Valid values are **1** (default) to **255. Routes with lower values receive higher preference in route selection.**

Defaults

If *distance* is not specified, the default value of 1 will be applied.

Mode

Global configuration: C3**(su)->router(Config)#**

Example

This example shows how to set IP address 10.1.2.3 as the next hop gateway to destination address 10.0.0.0:

```
C3(su)->router(Config)#ip route 10.0.0.0 255.0.0.0 10.1.2.3
```

ping

Use this command to test routing network connectivity by sending IP ping requests.

Syntax

ping *ip-address*

Parameters

ip-address	Specifies the IP address of the system to ping.

Defaults

None.

Mode

Privileged EXEC: C3(su)->router#

Usage

This command is also available in switch mode.

Examples

This example shows output from a successful ping to IP address 182.127.63.23:

```
C3(su)->router#ping 182.127.63.23
182.127.63.23 is alive
```

This example shows output from an unsuccessful ping to IP address 182.127.63.24:

```
C3(su)->router#ping 182.127.63.24
 no answer from 182.127.63.24
```

traceroute

Use this command to display a hop-by-hop path through an IP network from the device to a specific destination host. Three ICMP probes will be transmitted for each hop between the source and the traceroute destination.

Syntax

traceroute *host*

Parameters

host	Specifies a host to which the route of an IP packet will be traced.

Defaults

None.

Mode

Privileged EXEC: C3**(su)->router#**

Usage

There is also a traceroute command available in switch mode.

Example

This example shows how to use traceroute to display a round trip path to host 192.141.90.183.

```
C3(su)->router#traceroute 192.141.90.183
Traceroute to 192.141.90.183, 30 hops max, 40 byte packets
 1  10.1.56.1                0.000 ms           0.000 ms           0.000 ms
 2  10.1.48.254             10.000 ms           0.000 ms           0.000 ms
 3  10.1.0.2                 0.000 ms           0.000 ms           0.000 ms
 4  192.141.89.17            0.000 ms           0.000 ms          10.000 ms
 5  192.141.100.13           0.000 ms          10.000 ms           0.000 ms
 6  192.141.100.6            0.000 ms           0.000 ms          10.000 ms
 7  192.141.90.183           0.000 ms           0.000 ms           0.000 ms
```

Configuring ICMP Redirects

Purpose

Disable or enable sending ICMP redirect packets to the switch CPU for processing, at a global level and at an interface level. By default, sending ICMP redirects is enabled globally and on all interfaces. Disabling sending ICMP redirects can reduce CPU usage in certain deployments.

Commands

ip icmp redirect enable

Use this command to enable or disable sending ICMP redirects to the CPU for processing on a global level or on a specific interface. The **no** form of this command disables sending ICMP redirects to the CPU.

Syntax

```
ip icmp redirect enable
no ip icmp redirect enable
```

Parameters

None.

Defaults

By default, sending ICMP redirects to the CPU is enabled globally and on all interfaces.

Mode

Router global configuration mode: C3(su)->router(Config)#

Interface configuration mode: C3(su)->Router1(Config-if(Vlan 1))#

Usage

You can use this command in router global configuration mode to enable or disable sending ICMP redirects globally on the switch.

You can use this command in router interface configuration mode to enable or disable sending ICMP redirects only on specific interfaces.

Examples

This example disables sending ICMP redirects on the interface VLAN 5.

```
C3(su)->router#configure
C3(su)->router(Config)#interface vlan 5
C3(su)->Router1(Config-if(Vlan 5))# no ip icmp redirect enable
```

This example disables sending ICMP redirects globally.

```
C3(su)->router#configure
C3(su)->router(Config)#no ip icmp redirect enable
```

show ip icmp redirect

Use this command to display the status of sending ICMP redirects at a global or interface level.

Syntax

show ip icmp redirect {**status** | **interface** [**vlan** *vlan-id*]}

Parameters

status	Display the global ICMP redirect status.
interface	Display ICMP redirect status for interfaces.
vlan *vlan-id*	(Optional) Display ICMP redirect status for the specified VLAN.

Defaults

If no VLAN is specified with the **interface** parameter, information for all VLAN interfaces is displayed.

Mode

Privileged EXEC mode:C3(su)->router#

Router global configuration mode: C3(su)->router(Config)#

Examples

This example displays the global ICMP redirect status.

```
C3(su)->router#show ip icmp redirect status
Global ICMP Redirect status - Enabled
```

This example displays the ICMP redirect status for VLAN 5.

```
C3(su)->router#show ip icmp redirect interface vlan 5
Vlan Id                Admin Status
-------                ------------
5                      Enabled
```

20

IPv4 Routing Protocol Configuration

This chapter describes the IPv4 Routing Protocol Configuration set of commands and how to use them.

Router: The commands covered in this chapter can be executed only when the device is in router mode. For details on how to enable router configuration modes, refer to "Enabling Router Configuration Modes" on page 18-2.

Activating Advanced Routing Features

In order to enable advanced routing protocols, such as OSPF, DVMRP, VRRP, and PIM-SM, on a SecureStack C3 device, you must purchase and activate a license key. If you have purchased an advanced routing license, and have enabled routing on the device, you can activate your license as described in the chapter entitled "Activating Licensed Features."

If you are stacking your devices and require advanced routing features, all devices in the stack must have a valid license.

If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

Note: The command prompts used in examples throughout this guide show a system where the VLAN 1 interface has been configured for routing. The prompt changes depending on your current configuration mode, your specific device, and the interface types and numbers configured for routing on your system.

Configuring RIP

Purpose

To enable and configure the Routing Information Protocol (RIP).

RIP Configuration Task List and Commands

Table 20-1 lists the tasks and commands associated with RIP configuration. Commands are described in the associated section as shown.

Table 20-1 RIP Configuration Task List and Commands

To do this...	Use these commands...
Enable RIP configuration mode.	"router rip" on page 20-2
Enable RIP on an interface.	"ip rip enable" on page 20-3
Configure an administrative distance.	"distance" on page 20-3
Allow reception of a RIP version.	"ip rip send version" on page 20-4
Allow transmission of a RIP version.	"ip rip receive version" on page 20-5
Configure RIP simple authentication.	"ip rip authentication-key" on page 20-5
Configure RIP encrypted authentication.	"ip rip message-digest-key" on page 20-6
Disable automatic route summarization (necessary for enabling CIDR)	"no auto-summary" on page 20-7
Activate split horizon or poison-reverse.	"split-horizon poison" on page 20-7
Suppress sending routing updates.	"passive-interface" on page 20-8
Control reception of routing updates	"receive-interface" on page 20-9
Control advertising non-RIP routes.	"redistribute" on page 20-9

router rip

Use this command to enable or disable RIP configuration mode. The **no** form of this command disables RIP.

Syntax

```
router rip
no router rip
```

Parameters

None.

Defaults

None.

Mode

Global configuration: C3(su)->router(Config)#

Usage

You must execute the **router rip** command to enable the protocol before completing many RIP-specific configuration tasks. For details on enabling configuration modes, refer to Table 18-2 in "Enabling Router Configuration Modes" on page 18-2.

Example

This example shows how to enable RIP:

```
C3(su)->router#configure
C3(su)->router(Config)#router rip
C3(su)->router(Config-router)#
```

ip rip enable

Use this command to enable RIP on an interface. The **no** form of this command disables RIP on an interface: By default, RIP is disabled on all interfaces.

Syntax

```
ip rip enable
no ip rip enable
```

Parameters

None.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to enable RIP on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip rip enable
```

distance

Use this command to configure the administrative distance for RIP routes. The **no** form of this command resets RIP administrative distance to the default value of 120.

Syntax

```
distance weight
no distance [weight]
```

Parameters

weight	Specifies an administrative distance for RIP routes. Valid values are **1** - **255**.

Defaults

None.

Mode

Router configuration: C3(su)->router(Config-router)#

Usage

If several routes (coming from different protocols) are presented to the SecureStack C3, the protocol with the lowest administrative distance will be chosen for route installation. By default, RIP administrative distance is set to 120. The **distance** command can be used to change this value, resetting RIP's route preference in relation to other routes as shown in the table below.

Route Source	Default Distance
Connected	0
Static	1
OSPF	110
RIP	120

Example

This example shows how to change the default administrative distance for RIP to 1001:

```
C3(su)->router(Config)#router rip
C3(su)->router(Config-router)#distance 100
```

ip rip send version

Use this command to set the RIP version for RIP update packets transmitted out an interface. The **no** version of this command sets the version of the RIP update packets to RIPv1.

Syntax

```
ip rip send version {1 | 2 | r1compatible}
no ip rip send version
```

Parameters

1	Specifies RIP version 1. This is the default setting.
2	Specifies RIP version 2.
r1compatible	Specifies that packets be sent as version 2 packets, but transmits these as broadcast packets rather than multicast packets so that systems which only understand RIP version 1 can receive them.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the RIP send version to 2 for packets transmitted on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip rip send version 2
```

ip rip receive version

Use this command to set the RIP version(s) for RIP update packets accepted on an interface. The **no** version of this command sets the acceptable receive version of the RIP update packets to RIPv1.

Syntax

```
ip rip receive version {1 | 2 | 1 2 | none}
no ip rip receive version
```

Parameters

1	Specifies RIP version 1. This is the default setting.
2	Specifies RIP version 2.
1 2	Specifies RIP versions 1 and 2.
none	Specifies that no RIP routes will be processed on this interface.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Defaults

None.

Example

This example shows how to set the RIP receive version to 2 for update packets received on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip rip receive version 2
```

ip rip authentication-key

Use this command to enable or disable a RIP authentication key (password) for use on an interface. The **no** form of this command prevents RIP from using authentication.

Syntax

```
ip rip authentication-key name
no ip rip authentication-key
```

Parameters

name	Specifies the password to enable or disable for RIP authentication.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the RIP authentication key chain to "**password"** on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip rip authentication-key password
```

ip rip message-digest-key

Use this command to enable or disable a RIP MD5 authentication key (password) for use on an interface. The **no** form of this command prevents RIP from using authentication.

Syntax

ip rip message-digest-key *keyid* **md5** *key*
no ip rip message-digest-key *keyid*

Parameters

keyid	Specifies the key ID to enable or disable for RIP authentication. Valid values are **1** to **255**.
md5	Specifies use of the MD5 algorithm.
key	Specifies the RIP authentication password.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Defaults

None.

Examples

This example shows how to set the MD5 authentication ID to 5 for the RIP authentication key set on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip rip message-digest-key 5 md5 password
```

no auto-summary

Use this command to disable automatic route summarization.

Syntax

```
no auto-summary
auto-summary
```

Parameters

None.

Defaults

None.

Mode

Router configuration: C3**(su)->router(Config-router)#**

Usage

By default, RIP version 2 supports automatic route summarization, which summarizes subprefixes to the classful network boundary when crossing network boundaries. Disabling automatic route summarization enables CIDR, allowing RIP to advertise all subnets and host routing information on the SecureStack C3 device. To verify which routes are summarized for an interface, use the **show ip route** command as described in "show ip route" on page 19-19. The reverse of the command re-enables automatic route summarization. By default, RIP auto-summarization affects both RIPv1 and RIPv2 routes.

Note: This command is necessary for enabling CIDR for RIP on the SecureStack C3 device.

Example

This example shows how to disable RIP automatic route summarization:

```
C3(su)->router(Config)#router rip
C3(su)->router(Config-router)#no auto-summary
```

split-horizon poison

Use this command to enable or disable split horizon poison-reverse mode for RIP packets. The **no** form of this command disables split horizon poison reverse.

Syntax

```
split-horizon poison
no split-horizon poison
```

Parameters

None.

Defaults

None.

Mode

Router configuration: C3(su)->router(Config-router)#

Usage

Split horizon prevents a network from being advertised out the same interface it was received on. This function is disabled by default.

Example

This example shows how to disable split horizon poison reverse for RIP packets transmitted on the VLAN 1 interface:

```
C3(su)->router(Config)#router rip
C3(su)->Router1(Config-router)#no split-horizon poison
```

passive-interface

Use this command to prevent RIP from transmitting update packets on an interface. The **no** form of this command disables passive interface.

Syntax

passive-interface vlan *vlan-id*
no passive-interface vlan *vlan-id*

Parameters

vlan *vlan*-id	Specifies the number of the VLAN to make a passive interface. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.

Defaults

None.

Mode

Router configuration: C3(su)->router(Config-router)#

Usage

This command does not prevent RIP from monitoring updates on the interface.

Example

This example shows how to set VLAN 2 as a passive interface. No RIP updates will be transmitted on VLAN 2:

```
C3(su)->router(Config)#router rip
C3(su)->router(Config-router)#passive-interface vlan 2
```

receive-interface

Use this command to allow RIP to receive update packets on an interface. The **no** form of this command denies the reception of RIP updates. By default, receiving is enabled on all routing interfaces.

Syntax

```
receive-interface vlan vlan-id
no receive-interface vlan vlan-id
```

Parameters

vlan *vlan*-id	Specifies the number of the VLAN to make a receive interface. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.

Defaults

None.

Mode

Router configuration: C3(su)->router(Config-router)#

Usage

This command does not affect the sending of RIP updates on the specified interface.

Example

This example shows how to deny the reception of RIP updates on VLAN 2:

```
C3(su)->router(Config)#router rip
C3(su)->router(Config-router)#no receive-interface vlan 2
```

redistribute

Use this command to allow routing information discovered through non-RIP protocols to be distributed in RIP update messages. The **no** form of this command clears redistribution parameters.

Syntax

```
redistribute {connected | ospf process-id | static} [metric metric value]
[subnets]
no redistribute {connected | ospf process-id | static}
```

Parameters

connected	Specifies that non-RIP routing information discovered via directly connected interfaces will be redistributed.
ospf	Specifies that OSPF routing information will be redistributed in RIP.
process-id	Specifies the process ID, an internally used identification number for each instance of the OSPF routing process run on a router. Valid values are **1** to **65535**.

static	Specifies that non-RIP routing information discovered via static routes will be redistributed. Static routes are those created using the **ip route** command detailed in "ip route" on page 19-21.
metric *metric value*	(Optional) Specifies a metric for the connected, OSPF or static redistribution route. This value should be consistent with the designation protocol.
subnets	(Optional) Specifies that connected, OSPF or static routes that are subnetted will be redistributed.

Mode

Router configuration: C3(su)->router(Config-router)#

Defaults

If *metric value* is not specified, 1 will be applied.

If **subnets** is not specified, only non-subnetted routes will be redistributed.

Example

This example shows how to redistribute routing information discovered through static routes will be redistributed into RIP update messages:

```
C3(su)->router(Config)#router rip
C3(su)->router(Config-router)#redistribute static
```

Configuring OSPF

*** Advanced License Required ***

OSPF is an advanced routing feature that must be enabled with a license key. If you have purchased an advanced license key, and have enabled routing on the device, you must activate your license as described in the chapter entitiled "Activating Licensed Features" in order to enable the OSPF command set. If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

Purpose

To enable and configure the Open Shortest Path First (OSPF) routing protocol.

OSPF Configuration Task List and Commands

Table 20-2 lists the tasks and commands associated with OSPF configuration. Commands are described in the associated section as shown.

Table 20-2 OSPF Configuration Task List and Commands

To do this...	Use these commands...
If necessary, activate your advanced routing license.	See the "Activating Licensed Features" chapter.
Enable OSPF configuration mode.	"router id" on page 20-12
	"router ospf" on page 20-13
Enable or disable RFC 1583 compatibility.	"1583compatibility" on page 20-13
Configure OSPF Interface Parameters.	
Enable OSPF on the interface.	"ip ospf enable" on page 20-14
Configure an OSPF area.	"ip ospf areaid" on page 20-14
• Set the cost of sending a packet on an OSPF interface.	"ip ospf cost" on page 20-15
• Set a priority to help determine the OSPF designated router for the network.	"ip ospf priority" on page 20-15
• Adjust timers and message intervals.	"timers spf" on page 20-16
	"ip ospf retransmit-interval" on page 20-17
	"ip ospf transmit-delay" on page 20-17
	"ip ospf hello-interval" on page 20-18
	"ip ospf dead-interval" on page 20-18
• Configure OSPF authentication.	"ip ospf authentication-key" on page 20-19
	"ip ospf message digest key md5" on page 20-20
Configure OSPF Areas.	
• Configure an administrative distance.	"distance ospf" on page 20-20
• Define the range of addresses to be used by Area Boundary Routers (ABRs).	"area range" on page 20-21

Table 20-2 OSPF Configuration Task List and Commands (Continued)

To do this...	Use these commands...
• Define an area as a stub area.	"area stub" on page 20-22
• Set the cost value for the default route that is sent into a stub area.	"area default cost" on page 20-23
• Define an area as an NSSA.	"area nssa" on page 20-23
Create virtual links.	"area virtual-link" on page 20-24
Enable redistribution from non-OSPF routes.	"redistribute" on page 20-25
Monitor and maintain OSPF.	"show ip ospf" on page 20-26
	"show ip ospf neighbor" on page 20-30
	"show ip ospf interface" on page 20-28
	"show ip ospf neighbor" on page 20-30
	"show ip ospf virtual-links" on page 20-31
	"clear ip ospf process" on page 20-31

router id

Use this command to set the OSPF router ID for the device. This IP address must be set manually in order to run OSPF. The **no** form of this command removes the router ID for the device.

Syntax

```
router id ip-address
no router id
```

Parameters

ip-address	Specifies the IP address that OSPF will use as the router ID.

Defaults

None.

Mode

Global configuration: C3(su)->router(Config)#

Usage

This command sets the OSPF router ID. The OSPF area ID of a routed VLAN is configured on each interface with the interface command "ip ospf areaid" on page 20-14. If you do not configure an area ID on a routed interface running OSPF, the default area ID of 0.0.0.0 will be used.

Example

This example shows how to set the OSPF router ID to IP address 182.127.62.1:

```
C3(su)->router(Config-router)#router id 182.127.62.1
```

router ospf

Use this command to enable or disable Open Shortest Path First (OSPF) configuration mode. The **no** form of this command disables OSPF configuration mode.

Syntax

```
router ospf process-id
no router ospf process-id
```

Parameters

process-id	Specifies the process ID, an internally used identification number for an OSPF routing process run on a router. Only one OSPF process is allowed per stack or standalone. Valid values are **1** to **65535**.

Defaults

None.

Mode

Global configuration: C3(su)->router(Config)#

Usage

You must execute the **router ospf** command to enable the protocol before completing many OSPF-specific configuration tasks. For details on enabling configuration modes, refer to Table 18-2 on page 18-2.

Only one OSPF process (*process-id*) is allowed per SecureStack C3 router.

Example

This example shows how to enable routing for OSPF process 1:

```
C3(su)->router#conf terminal
C3(su)->router(Config)#router ospf 1
C3(su)->router(Config-router)#
```

1583compatibility

Use this command to enable RFC 1583 compatibility on OSPF interfaces. The **no** form of this command disables RFC 1583 compatibility on OSPF interfaces.

Syntax

```
1583compatability
no 1583compatability
```

Parameters

None.

Defaults

None.

Mode

Router configuration: C3**(su)->router(Config-router)#**

Example

This example shows how to enable RFC 1583 compatibility:

```
C3(su)->router(Config)#router ospf 1
C3(su)->router(Config-router)#1583compatability
```

ip ospf enable

Use this command to enable OSPF on an interface. The **no** form of this command disables OSPF on an interface.

Syntax

```
ip ospf enable
no ip ospf enable
```

Parameters

None.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to enable OSPF on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip ospf enable
```

ip ospf areaid

Use this command to configure area IDs for OSPF interfaces. If OSPF is enabled on an interface as described in "ip ospf enable" on page 20-14, the OSPF area will default to 0.0.0.0. The **no** form of this command removes OSPF routing for the interfaces.

Syntax

```
ip ospf areaid area-id
no ip ospf areaid
```

Parameters

area-id	Specifies the *area-id* to be associated with the OSPF interface. Valid values are decimal values or IP addresses.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to configure the VLAN 1 interface as area 0.0.0.31:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip ospf areaid 0.0.0.31
```

ip ospf cost

Use this command to set the cost of sending an OSPF packet on an interface. The **no** form of this command resets the OSPF cost to the default of 10.

Syntax

ip ospf cost *cost*
no ip ospf cost

Parameters

cost	Specifies the cost of sending a packet. Valid values range from **1** to **65535**.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

Each router interface that participates in OSPF routing is assigned a default cost. This command overwrites the default of 10.

Example

This example shows how to set the OSPF cost to 20 for the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip ospf cost 20
```

ip ospf priority

Use this command to set the OSPF priority value for router interfaces. The **no** form of this command resets the value to the default of 1.

Syntax

ip ospf priority ***number***
no ip ospf priority

Parameters

number	Specifies the router's OSPF priority in a range from **0** to **255**. Default value is 1.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

The priority value is communicated between routers by means of hello messages and influences the election of a designated router.

Example

This example shows how to set the OSPF priority to 20 for the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip ospf priority 20
```

timers spf

Use this command to change OSPF timer values to fine-tune the OSPF network. The **no** form of this command restores the default timer values (5 seconds for delay and 10 seconds for holdtime).

Syntax

timers spf *spf-delay spf-hold*
no timers spf

Parameters

spf-delay	Specifies the delay, in seconds, between the receipt of an update and the SPF execution. Valid values are **0** to **4294967295**.
spf-hold	Specifies the minimum amount of time, in seconds, between two consecutive OSPF calculations. Valid values are **0** to **4294967295**. A value of 0 means that two consecutive OSPF calculations are performed one immediately after the other.

Defaults

None.

Mode

Router configuration: C3**(su)->router(Config-router)#**

Example

This example shows how to set SPF delay time to 7 seconds and hold time to 3:

```
C3(su)->router(Config)#router ospf 1
C3(su)->router(Config-router)#timers spf 7 3
```

ip ospf retransmit-interval

Use this command to set the amount of time between retransmissions of link state advertisements (LSAs) for adjacencies that belong to an interface. The **no** form of this command resets the retransmit interval value to the default, 5 seconds.

Syntax

```
ip ospf retransmit-interval seconds
no ip ospf retransmit-interval
```

Parameters

seconds	Specifies the retransmit time in seconds. Valid values are **1** to **65535**.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the OSPF retransmit interval for the VLAN 1 interface to 20:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip ospf retransmit-interval 20
```

ip ospf transmit-delay

Use this command to set the amount of time required to transmit a link state update packet on an interface. The **no** form of this command resets the retransmit interval value to the default, 1 second.

Syntax

```
ip ospf transmit-delay seconds
no ip ospf transmit-delay
```

Parameters

seconds	Specifies the transmit delay in seconds. Valid values are from **1** to **65535**.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the time required to transmit a link state update packet on the VLAN 1 interface at 20 seconds:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip ospf transmit-delay 20
```

ip ospf hello-interval

Use this command to set the number of seconds a router must wait before sending a hello packet to neighbor routers on an interface. The **no** form of this command sets the hello interval value to the default value of 10 seconds.

Syntax

```
ip ospf hello-interval seconds
no ip ospf hello-interval
```

Parameters

seconds	Specifies the hello interval in seconds. Hello interval must be the same on neighboring routers (on a specific subnet), but can vary between subnets. This parameter is an unsigned integer with valid values between **1** and **65535**.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the hello interval to 5 for the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip ospf hello-interval 5
```

ip ospf dead-interval

Use this command to set the number of seconds a router must wait to receive a hello packet from its neighbor before determining that the neighbor is out of service. The **no** form of this command sets the dead interval value to the default value of 40 seconds.

Syntax

```
ip ospf dead-interval seconds
no ip ospf dead-interval
```

Parameters

seconds	Specifies the number of seconds that a router must wait to receive a hello packet before declaring the neighbor as "dead" and removing it from the OSPF neighbor list. Dead interval must be the same on neighboring routers (on a specific subnet), but can vary between subnets. This parameter is an unsigned integer ranging from **1** to **65535**. Default value is 40 seconds.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the dead interval to 20 for the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip ospf dead-interval 20
```

ip ospf authentication-key

Use this command to assign a password to be used by neighboring routers using OSPF's simple password authentication.The **no** form of this command removes an OSPF authentication password on an interface.

Syntax

ip ospf authentication-key *password*
no ip ospf authentication-key

Parameters

password	Specifies an OSPF authentication password. Valid values are alphanumeric strings up to 8 characters in length.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

This password is used as a "key" that is inserted directly into the OSPF header in routing protocol packets. A separate password can be assigned to each OSPF network on a per-interface basis.

All neighboring routers on the same network must have the same password configured to be able to exchange OSPF information.

Example

This example shows how to enables an OSPF authentication key on the VLAN 1 interface with the password "yourpass":

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip ospf authentication-key yourpass
```

ip ospf message digest key md5

Use this command to enable or disable OSPF MD5 authentication on an interface. This validates OSPF MD5 routing updates between neighboring routers. The **no** form of this command disables MD5 authentication on an interface.

Syntax

```
ip ospf message-digest-key keyid md5 key
no ip ospf message-digest-key keyid
```

Parameters

keyid	Specifies the key identifier on the interface where MD5 authentication is enabled. Valid values are integers from **1** to **255**.
key	Specifies a password for MD5 authentication to be used with the *keyid*. Valid values are alphanumeric strings of up to 16 characters.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to enable OSPF MD5 authentication on the VLAN 1 interface, set the key identifier to 20, and set the password to "passone":

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip ospf message-digest-key 20 md5 passone
```

distance ospf

Use this command to configure the administrative distance for OSPF routes. The **no** form of this command resets OSPF administrative distance to the default values.

Syntax

```
distance ospf {external | inter-area | intra-area} weight
no distance ospf {external | inter-area | intra-area}
```

Parameters

external | **inter-area** | **intra-area**	Applies the distance value to external (type 5 and type 7), to inter-area, or to intra-area routes. **Note:** The value for intra-area distance must be less than the value for inter-area distance, which must be less than the value for external distance.
weight	Specifies an administrative distance for OSPF routes. Valid values are **1** - **255**.

Defaults

If route type is not specified, the distance value will be applied to all OSPF routes.

Mode

Router configuration: C3**(su)->router(Config-router)#**

Usage

If several routes (coming from different protocols) are presented to the SecureStack C3, the protocol with the lowest administrative distance will be chosen for route installation. By default, OSPF administrative distance is set to 110. The **distance ospf** command can be used to change this value, resetting OSPF's route preference in relation to other routes as shown in the table below.

Route Source	Default Distance
Connected	0
Static	1
OSPF	Intra-area - 8; Inter-area - 10; External type 1 - 13; External type 2 - 150
RIP	15

Example

This example shows how to change the default administrative distance for external OSPF routes to 100:

```
C3(su)->router(Config)#router ospf 1
C3(su)->router(Config-router)#distance ospf external 100
```

area range

Use this command to define the range of addresses to be used by Area Border Routers (ABRs) when they communicate routes to other areas. Each SecureStack C3 stack can support up to 4 OSPF areas. The **no** form of this command stops the routes from being summarized.

Syntax

area *area-id* **range** *ip-address ip-mask* [**advertise** | **no-advertise**]
no area ***area-id*** **range** *ip-address ip-mask*

Parameters

*area-i*d	Specifies the area from which routes are to be summarized. This is a decimal value from 0 to 429496295.
ip-address	Specifies the IP address associated with the area ID.
ip-mask	Specifies the mask for the IP address.
advertise | **no-advertise**	(Optional) Enters address range in advertise mode, or do not advertise mode.

Defaults

If not specified, **advertise** mode will be set.

Mode

Router configuration: C3**(su)->router(Config-router)#**

Example

This example shows how to define the address range as 172.16.0.0/16 for summarized routes from area 0.0.0.8:

```
C3(su)->router(Config)#router ospf 1
C3(su)->router(Config-router)#area 0.0.0.8 range 172.16.0.0 255.255.0.0
```

area stub

Use this command to define an OSPF area as a stub area. This is an area into which Autonomous System external ASAs will not be flooded. The **no** form of this command changes the stub back to a plain area.

Syntax

area *area-id* **stub** [**no-summary**]
no area ***area-id*** **stub** [*no-summary*]

Parameters

area-id	Specifies the stub area. Valid values are decimal values or ip addresses.
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending Link State Advertisements (LSAs) into the stub area. When this parameter is used, it means that all destinations outside of the stub area are represented by means of a default route.

Mode

Router configuration: C3**(su)->router(Config-router)#**

Defaults

If **no-summary** is not specified, the stub area will be able to receive LSAs.

Example

The following example shows how to define OSPF area 10 as a stub area:

```
C3(su)->router(Config)#router ospf 1
C3(su)->router(Config-router)#area 10 stub
```

area default cost

Use this command to set the cost value for the default route that is sent into a stub area and NSSA by an Area Border Router (ABR). The **no** form of this command removes the cost value from the summary route that is sent into the stub area.

Syntax

area *area-id* **default-cost** *cost*
no area *area-id* **default-cost**

Parameters

area-id	Specifies the stub area. Valid values are decimal values or IP addresses.
cost	Specifies a cost value for the summary route that is sent into a stub area by default. Valid values are 24-bit numbers, from **0** to **16777215**.

Defaults

None.

Mode

Router configuration: C3**(su)->router(Config-router)#**

Usage

The use of this command is restricted to ABRs attached to stub and NSSA areas.

Example

This example shows how to set the cost value for stub area 10 to 99:

```
C3(su)->router(Config)#router ospf 1
C3(su)->router(Config-router)#area 10 default-cost 99
```

area nssa

Use this command to configure an area as a Not So Stubby Area (NSSA). The **no** form of this command changes the NSSA back to a plain area.

Syntax

area *area-id* **nssa [default-information-originate]**
no area ***area-id*** **nssa [default-information-originate]**

Parameters

area-id	Specifies the NSSA area. Valid values are decimal values or IP addresses.
default-information-originate	(Optional) Generates a default of Type 7 into the NSSA. This is used when the router is an NSSA ABR.

Defaults

If **default-information-originate** is not specified, no default type will be generated.

Mode

Router configuration: C3(su)->router(Config-router)#

Usage

An NSSA allows some external routes represented by external Link State Advertisements (LSAs) to be imported into it. This is in contrast to a stub area that does not allow any external routes. External routes that are not imported into an NSSA can be represented by means of a default route. This configuration is used when an OSPF internetwork is connected to multiple non-OSPF routing domains.

Example

This example shows how to configure area 10 as an NSSA area:

```
C3(su)->router(Config)#router ospf 1
C3(su)->router(Config-router)#area 10 nssa default-information-originate
```

area virtual-link

Use this command to define an OSPF virtual link, which represents a logical connection between the backbone and a non-backbone OSPF area. The **no** form of this command removes the virtual link and/or its associated settings.

Syntax

area *area-id* **virtual-link** *router-id*
no area *area-id* **virtual-link** *router-id*

In addition to the syntax above, the options for using this command are:

area *area-id* **virtual-link** *router-id* **authentication-key** *key*
no area *area-id* **virtual-link** *router-id* **authentication-key** *key*

area *area-id* **virtual-link** *router-id* **dead-interval** *seconds*
no area *area-id* **virtual-link** *router-id* **dead-interval** *seconds*

area *area-id* **virtual-link** *router-id* **hello-interval** *seconds*
no area *area-id* **virtual-link** *router-id* **hello-interval** *seconds*

area *area-id* **virtual-link** *router-id* **retransmit-interval** *seconds*
no area *area-id* **virtual-link** *router-id* **retransmit-interval** *seconds*

area *area-id* **virtual-link** *router-id* **transmit-delay** *seconds*
no area *area-id* **virtual-link** *router-id* **transmit-delay** *seconds*

Parameters

area-id	Specifies the transit area for the virtual link. Valid values are decimal values or IP addresses. A transit area is an area through which a virtual link is established.
router-id	Specifies the router ID of the virtual link neighbor.
authentication-key *key*	Specifies a password to be used by the virtual link. Valid values are alphanumeric strings of up to 8 characters. Neighbor virtual link routers on a network must have the same password.
dead-interval *seconds*	Specifies the number of seconds that a router must wait to receive a hello packet before declaring the neighbor as "dead" and removing it from the OSPF neighbor list. This value must be the same for all virtual links attached to a certain subnet, and it is a value ranging from **1** to **8192**.
hello-interval *seconds*	Specifies the number of seconds between hello packets on the virtual link. This value must be the same for all virtual links attached to a network and it is a value ranging from **1** to **8192**.
retransmit-interval *seconds*	Specifies the number of seconds between successive retransmissions of the same LSAs. Valid values are greater than the expected amount of time required for the update packet to reach and return from the interface, and range from **1** to **8192**. Default is 5 seconds.
transmit-delay *seconds*	Specifies the estimated number of seconds before a link state update packet on the interface to be transmitted. Valid values range from **1** to **8192**. Default is 1 second.

Defaults

None.

Mode

Router configuration: C3(su)->router(Config-router)#

Example

This example shows how to configure a virtual link over transition area 0.0.0.2 to router ID 192.168.7.2:

```
C3(su)->router(Config)#router ospf 1
C3(su)->router(Config-router)#area 0.0.0.2 virtual-link 192.168.7.2
```

redistribute

Use this command to allow routing information discovered through non-OSPF protocols to be distributed in OSPF update messages. The **no** form of this command clears redistribution parameters.

Syntax

redistribute {connected | **rip** | **static**} [**metric** *metric value*] [**metric-type** *type-value*] [**subnets**]
no redistribute {**connected** | **rip** | **static**}

Parameters

connected	Specifies that non-OSPF information discovered via directly connected interfaces will be redistributed.
rip	Specifies that RIP routing information will be redistributed in OSPF.
static	Specifies that non-OSPF information discovered via static routes will be redistributed. Static routes are those created using the **ip route** command detailed in "ip route" on page 19-21.
metric *metric value*	(Optional) Specifies a metric for the connected, RIP or static redistribution route. This value should be consistent with the designation protocol.
metric-type *type value*	(Optional) Specifies the external link type associated with the default connected, RIP or static route advertised into the OSPF routing domain. Valid values are **1** for type 1 external route, and **2** for type 2 external route.
subnets	(Optional) Specifies that connected, RIP, or static routes that are subnetted routes will be redistributed.

Defaults

If *metric value* is not specified, 0 will be applied.

If *type value* is not specified, type 2 (external route) will be applied.

If **subnets** is not specified, only the shortest prefix matching routes will be redistributed.

Mode

Router configuration: C3(su)->router(Config-router)#

Example

This example shows how to redistribute RIP routing information to non-subnetted routes in OSPF routes:

```
C3(su)->router(Config)#router ospf
C3(su)->router(Config-router)#redistribute rip
```

show ip ospf

Use this command to display OSPF information.

Syntax

show ip ospf

Parameters

None.

Defaults

None.

Mode

Any router mode.

Example

This example shows how to display OSPF information:

```
C3(su)->router#show ip ospf
Routing process "ospf 1" with ID 155.155.155.155
Supports only Normal TOS route.
It is not an area border router and is an autonomous system boundary router.
Redistributing External Routes from static
Number of areas in this router is 2
Area 0.0.0.0
     SPF algorithm executed 0 times
     Area ranges are
     Link State Age Interval is 10
Area 0.0.0.8
     SPF algorithm executed 302 times
     Area ranges are
     Link State Age Interval is 10
```

show ip ospf database

Use this command to display the OSPF link state database.

Syntax

show ip ospf database

Parameters

None.

Defaults

None.

Mode

Any router mode.

Example

This example shows how to display all OSPF link state database information. This is a portion of the command output:

```
C3(su)->router#show ip ospf database
OSPF Router with ID(155.155.155.155)

           Displaying Ipnet Sum Link States(Area 0.0.0.0)
 LinkID           ADV Router       Age       Seq#             Checksum
192.168.16.0      155.155.155.155  1751      0x80000036       0x18a

           Displaying As External Link States(Area 0.0.0.0)
 LinkID           ADV Router       Age       Seq#             Checksum
191.2.2.0         155.155.155.155  1306      0x8000003c       0x9096
191.3.3.3         155.155.155.155  1306      0x8000003c       0x5bc6
191.3.3.4         155.155.155.155  1306      0x8000003c       0x51cf
191.3.3.5         155.155.155.155  1306      0x8000003c       0x47d8
191.3.3.6         155.155.155.155  1307      0x8000003c       0x3de1
191.3.3.7         155.155.155.155  1307      0x8000003c       0x33ea
191.3.3.8         155.155.155.155  1307      0x8000003c       0x29f3
191.3.3.9         155.155.155.155  1307      0x8000003c       0x1ffc
```

```
191.4.0.0         155.155.155.155  1307      0x8000003c       0x8e98

          Displaying Router Link States(Area 0.0.0.8)
 LinkID           ADV Router       Age       Seq#             Checksum
3.3.3.3           3.3.3.3          986       0x8000008e       0xb6f9
155.155.155.155   155.155.155.155  977       0x8000009c       0x6e96

          Displaying Net Link States(Area 0.0.0.8)
 LinkID           ADV Router       Age       Seq#             Checksum
192.168.30.2      155.155.155.155  310       0x8000003b       0x59ab
192.168.31.2      155.155.155.155  997       0x80000002       0xc07c
192.168.32.2      155.155.155.155  997       0x80000002       0xb586
192.168.33.2      155.155.155.155  998       0x80000002       0xaa90
          Displaying Ipnet Sum Link States(Area 0.0.0.8)
 LinkID           ADV Router       Age       Seq#             Checksum
0.0.0.0           3.3.3.3          361       0x80000005       0x311d
8.1.1.0           3.3.3.3          1512      0x80000003       0x3de1
8.1.2.0           3.3.3.3          1512      0x80000003       0x32eb
8.1.3.0           3.3.3.3          1502      0x80000003       0x27f5
8.1.4.0           3.3.3.3          1512      0x80000003       0x1c00
```

Table 20-3 provides an explanation of the command output.

Table 20-3 show ip ospf database Output Details

Output Field	What It Displays...
Link ID	Link ID, which varies as a function of the link state record type, as follows: • Net Link States - Shows the interface IP address of the designated router to the broadcast network. • Router Link States - Shows the ID of the router originating the record. • Summary Link States - Shows the summary network prefix.
ADV Router	Router ID of the router originating the link state record.
Age	Age (in seconds) of the link state record.
Seq#	OSPF sequence number assigned to each link state record.
Checksum	Field in the link state record used to verify the contents upon receipt by another router.
LinkCount	Link count of router link state records. This number is equal to, or greater than, the number of active OSPF interfaces on the originating router.

show ip ospf interface

Use this command to display OSPF interface related information, including network type, priority, cost, hello interval, and dead interval.

Syntax

show ip ospf interface [**vlan** *vlan-id*]

Parameters

vlan *vlan*-id	(Optional) Displays OSPF information for a specific VLAN. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.

Defaults

If *vlan-id* is not specified, OSPF statistics will be displayed for all VLANs.

Mode

Any router mode.

Example

This example shows how to display all OSPF related information for the VLAN 6 interface:

```
C3(su)->router#show ip ospf interface vlan 6
Vlan 6
Internet Address 192.168.6.2  Mask 255.255.255.0, Area 0.0.0.0
Router ID 3.3.3.3 , Cost: 10  (computed)
Transmit Delay is 1 sec , State designated-router , Priority 1
Designated Router id 3.3.3.3 , Interface Addr 192.168.6.2
Backup Designated Router id 2.2.2.2 ,
Timer intervals configured ,   Hello 10 , Dead 40 , Retransmit 5
```

Table 20-4 provides an explanation of the command output.

Table 20-4 show ip ospf interface Output Details

Output Field	What It Displays...
Vlan	VLAN ID
Internet Address	IP address and mask assigned to this interface.
Area	Area ID
Router ID	Router ID configured on this router.
Cost	OSPF interface cost, which is either default, or assigned with the **ip ospf cost** command. For details, refer to "ip ospf cost" on page 20-15.
Transmit Delay	The number (in seconds) added to the LSA (Link State Advertisement) age field.
State	The interface state (versus the state between neighbors). Valid values include Backup Designated Router, Designated Router, and Err for error.
Priority	The interface priority value, which is either default, or assigned with the **ip ospf priority** command. For details, refer to "ip ospf priority" on page 20-15.
Designated Router id	The router ID of the designated router on this subnet, if one exists, in which case Err will be displayed.
Interface Addr	IP address of the designated router on this interface.
Backup Designated Router id	IP address of the backup designated router on this interface, if one exists, in which case Err will be displayed.
Timer intervals configured	OSPF timer intervals. These are either default, or configured with the **ip ospf retransmit-interval** ("ip ospf retransmit-interval" on page 20-17), the **ip ospf hello-interval** ("ip ospf hello-interval" on page 20-18), the **ip ospf retransmit-delay** ("ip ospf transmit-delay" on page 20-17) and the **ip ospf dead interval** ("ip ospf dead-interval" on page 20-18) commands.

show ip ospf neighbor

Use this command to display the state of communication between an OSPF router and its neighbor routers.

Syntax

show ip ospf neighbor [**detail**] [*ip-address*] [**vlan** *vlan-id*]

Parameters

detail	(Optional) Displays detailed information about the neighbors, including the area in which they are neighbors, who the designated router/backup designated router is on the subnet, if applicable, and the decimal equivalent of the E-bit value from the hello packet options field.
ip-address	(Optional) Displays OSPF neighbors for a specific IP address.
vlan *vlan*-id	(Optional) Displays OSPF neighbors for a specific VLAN. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.

Defaults

If **detail** is not specified, summary information will be displayed.

If *ip-address* is not specified, OSPF neighbors will be displayed for all IP addresses configured for routing.

If *vlan-id* is not specified, OSPF neighbors will be displayed for all VLANs configured for routing.

Mode

Any router mode.

Example

This example shows how to use the **show ospf neighbor** command:

```
C3(su)->router#show ip ospf neighbor
ID              Pri    State     Dead-Int  Address       Interface
182.127.62.1      1    FULL      40        182.127.63.1  vlan1
```

Table 20-5 provides an explanation of the command output.

Table 20-5 show ip ospf neighbor Output Details

Output Field	What It Displays...
ID	Neighbor's router ID of the OSPF neighbor.
Pri	Neighbor's priority over this interface.
State	Neighbor's OSPF communication state.
Dead-Int	Interval (in seconds) this router will wait without receiving a Hello packet from a neighbor before declaring the neighbor is down.
Address	Neighbor's IP address.
Interface	Neighbor's interface (VLAN).

show ip ospf virtual-links

Use this command to display information about the virtual links configured on a router. A virtual link represents a logical connection between the backbone and a non-backbone OSPF area.

Syntax

show ip ospf virtual-links

Parameters

None.

Defaults

None.

Mode

Any router mode.

Example

This example shows how to display OSPF virtual links information:

```
C3(su)->router#show ip ospf virtual-links
Neighbor ID 155.155.155.155
 Transit area 0.0.0.8
 Transmit delay is 1 sec State point-to-point
 Timer intervals configured:
               Hello 10, Dead 40, Retransmit 5
 Adjacency State Full
```

Table 20-6 provides an explanation of the command output.

Table 20-6 show ip ospf virtual links Output Details

Output Field	What It Displays...
Neighbor ID	ID of the virtual link neighbor, and the virtual link status, which is up or down.
Transit area	ID of the transit area through which the virtual link is configured.
Transmit delay	Amount of time required to transmit a link state update packet on an interface.
State	Whether the state of this interface is down or point-to-point.
Timer intervals configured	Timer intervals configured for the virtual link, including Hello, Wait, and Retransmit intervals.
Adjacency State	State of adjacency between this router and the virtual link neighbor of this router.

clear ip ospf process

Use this command to reset the OSPF process. This will require adjacencies to be reestablished and routes to be reconverged.

Syntax

clear ip ospf process *process-id*

Parameters

process-id	Specifies the process ID, an internally used identification number for each instance of the OSPF routing process run on a router. Valid values are **1** to **65535**.

Defaults

None.

Mode

Privileged EXEC: C3(su)->router#

Example

This example shows how to reset OSPF process 1:

```
C3(su)->router#clear ip ospf process 1
```

Configuring DVMRP

*** Advanced License Required ***

DVMRP is an advanced routing feature that must be enabled with a license key. If you have purchased an advanced license key, and have enabled routing on the device, you must activate your license as described in the chapter entitled “Activating Licensed Features” in order to enable the DVMRP command set. If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

Note: An Enterasys Networks Feature Guide document containing an in-depth discussion of multicast configuration is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

Purpose

To enable and configure the Distance Vector Multicast Routing Protocol (DVMRP) on an interface. DVMRP routes multicast traffic using a technique known as Reverse Path Forwarding. When a router receives a packet, it floods the packet out of all paths except the one that leads back to the packet’s source. Doing so allows a data stream to reach all VLANs (possibly multiple times). If a router is attached to a set of VLANs that do not want to receive from a particular multicast group, the router can send a “prune” message back up the distribution tree to stop subsequent packets from traveling where there are no members. DVMRP will periodically reflood in order to reach any new hosts that want to receive from a particular group.

Note: IGMP must be enabled on all VLANs running DVMRP, and must also be globally enabled on the SecureStack C3. For details on enabling IGMP, refer to Chapter 13.

Commands

For information about...	Refer to page...
ip dvmrp	20-34
ip dvmrp enable	20-34
ip dvmrp metric	20-35
show ip dvmrp	20-35

See also show ip mroute on page 20-59, which can be used to display the IP multicast routing table.

Enabling DVMRP on an Interface

DVMRP is disabled by default, both globally and on each interface. Enabling DVMRP on a routed interface requires completing the steps listed in Table 20-1.

Table 20-1 Commands to Enable DVMRP on an Interface

To do this...	Use these commands...
Globally enable IGMP.	“ip igmp” on page 13-10
Globally enable DVMRP.	“ip dvmrp” on page 20-34.
Enable IGMP on each interface.	“ip igmp enable” on page 13-11
Enable DVMRP on each interface .	“ip dvmrp enable” on page 20-34

ip dvmrp

Use this command to enable the DVMRP process. The **no** form of this command disables the DVMRP process:

Syntax

```
ip dvmrp
no ip dvmrp
```

Parameters

None.

Defaults

None.

Mode

Global configuration: C3(su)->router(Config)#

Example

This example shows how to enable the DVMRP process:

```
C3(su)->router(Config)#ip dvmrp
```

ip dvmrp enable

Use this command to enable DVMRP on an interface. The **no** form of this command disables DVMRP on an interface:

Syntax

```
ip dvmrp enable
no ip dvmrp enable
```

Parameters

None.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to enable DVMRP on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip dvmrp enable
```

ip dvmrp metric

Use this command to configure the metric associated with a set of destinations for DVMRP reports.

Syntax

ip dvmrp metric *metric*

Parameters

metric	Specifies a metric associated with a set of destinations for DVMRP reports. Valid values are from **1** to **31**.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

To reset the DVMRP metric back to the default value of 1, enter **ip dvmrp metric 1**.

Example

This example shows how to set a DVMRP of 16 on the VLAN 1 interface:

```
C3(su)->router(Config-if(Vlan 1))#ip dvmrp metric 16
```

show ip dvmrp

Use this command to display DVMRP routing information.

Syntax

show ip dvmrp [**route** | **neighbor** | **status**]

Parameters

route | **neighbor** | **status**	(Optional) Displays, DVMRP routing information, neighbor information, or DVMRP enable status.

Defaults

If no optional parameters are specified, status information will be displayed.

Mode

Any router mode.

Example

This example shows how to display DVMRP status information:

```
C3(su)->router#show ip dvmrp
Vlan Id     Metric     Admin Status    Oper. Status
-------     -------    ------------    ------------
10                     Enabled         Enabled
18                     Enabled         Enabled
20                     Enabled         Enabled
25                     Enabled         Enabled
32                     Enabled         Enabled
500                    Enabled         Disabled
```

Configuring IRDP

Purpose

To enable and configure the ICMP Router Discovery Protocol (IRDP) on an interface. This protocol enables a host to determine the address of a router it can use as a default gateway. It is disabled by default.

Commands

ip irdp enable

Use this command to enable IRDP on an interface. The **no** form of this command disables IRDP on an interface.

Syntax

```
ip irdp enable
no ip irdp enable
```

Parameters

None.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to enable IRDP on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip irdp enable
```

ip irdp maxadvertinterval

Use this command to set the maximum interval in seconds between IRDP advertisements. The **no** form of this command resets the maximum advertisement interval to the default value of **600** seconds.

Syntax

```
ip irdp maxadvertinterval interval
no irdp maxadvertinterval
```

Parameters

interval	Specifies a maximum advertisement interval in seconds. Valid values are **4** to **1800**.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the maximum IRDP advertisement interval to 1000 seconds on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip irdp maxadvertinterval 1000
```

ip irdp minadvertinterval

Use this command to set the minimum interval in seconds between IRDP advertisements. The **no** form of this command deletes the custom holdtime setting, and resets the minimum advertisement interval to the default value of three-fourths of the **maxadvertinterval** value, which is equal to 450 seconds.

Syntax

```
ip irdp minadvertinterval interval
no irdp minadvertinterval
```

Parameters

interval	Specifies a minimum advertisement interval in seconds. Valid values are **3** to **1800**.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the minimum IRDP advertisement interval to 500 seconds on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip irdp minadvertinterval 500
```

ip irdp holdtime

Use this command to set the length of time in seconds IRDP advertisements are held valid. The **no** form of this command resets the hold time to the default value of three times the **maxadvertinterval** value, which is equal to 1800 seconds.

Syntax

```
ip irdp holdtime holdtime
no irdp holdtime
```

Parameters

holdtime	Specifies the hold time in seconds. Valid values are **0** to **9000.**

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the IRDP hold time to 4000 seconds on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip irdp holdtime 4000
```

ip irdp preference

Use this command to set the IRDP preference value for an interface. This value is used by IRDP to determine the interface's selection as a default gateway address. The **no** form of this command resets the interface's IRDP preference value to the default of **0**.

Syntax

```
ip irdp preference preference
no irdp preference
```

Parameters

preference	Specifies the value to indicate the interface's use as a default router address. Valid values are **-2147483648** to **2147483647**. The minimum value indicates that the address, even though it may be advertised, is not to be used by neighboring hosts as a default router address.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set IRDP preference on the VLAN 1 interface so that the interface's address may still be advertised, but cannot be used by neighboring hosts as a default router address:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip irdp preference -2147483648
```

ip irdp broadcast

Use this command to configure IRDP to use the limited broadcast address of 255.255.255.255. The default is multicast with address 224.0.0.1. The **no** form of this command resets IRDP to use multicast on IP address 224.0.0.1.

Syntax

```
ip irdp broadcast
no ip irdp broadcast
```

Parameters

None.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to enable broadcast for IRDP on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip irdp broadcast
```

show ip irdp

Use this command to display IRDP information.

Syntax

```
show ip irdp [vlan vlan-id]
```

Parameters

vlan *vlan-id*	(Optional) Displays IRDP information for a specific VLAN. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.

Defaults

If **vlan** *vlan-id* is not specified, IRDP information for all interfaces will be displayed.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to display IRDP information for the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(vlan 1))#show ip irdp vlan 1
Interface vlan 1 has router discovery enabled
Advertisements will occur between 450 and 600 seconds
Advertisements are sent with broadcasts
Advertisements are valid for 1800 seconds
Default preference will be 0
```

Configuring VRRP

*** Advanced License Required ***

VRRP is an advanced routing feature that must be enabled with a license key. If you have purchased an advanced license key, and have enabled routing on the device, you must activate your license as described in the chapter entitled “Activating Licensed Features” in order to enable the VRRP command set. If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

Purpose

To enable and configure the Virtual Router Redundancy Protocol (VRRP). This protocol eliminates the single point of failure inherent in the static default routed environment by transferring the responsibility from one router to another if the original router goes down. VRRP-enabled routers decide who will become master and who will become backup in the event the master fails.

Commands

router vrrp

Use this command to enable or disable VRRP configuration mode. The **n**o form of this command removes all VRRP configurations from the running configuration.

Syntax

```
router vrrp
no router vrrp
```

Parameters

None.

Defaults

None.

Mode

Global configuration: C3(su)->router(Config)#

Usage

You must execute the **router vrrp** command to enable the protocol before completing other VRRP-specific configuration tasks. For details on enabling configuration modes, refer to Table 18-2 on page 18-2.

Example

This example shows how enable VRRP configuration mode:

```
C3(su)->router#configure
C3(su)->router(Config)#router vrrp
C3(su)->router(Config-router)#
```

create

Use this command to create a VRRP session. Each SecureStack C3 system supports up to 20 VRRP sessions. The **no** form of this command disables the VRRP session.

Syntax

create vlan *vlan-id vrid*
no create vlan *vlan-id vrid*

Parameters

vlan *vlan*-id	Specifies the number of the VLAN on which to create a VRRP session. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.
vrid	Specifies a unique Virtual Router ID (VRID) to associate with the routing interface.

Defaults

None.

Mode

`Router configuration: C3(su)->router(Config-router)#`

Usage

This command must be executed to create an instance of VRRP on a routing interface (VLAN) before any other VRRP settings can be configured.

Example

This example shows how to create a VRRP session on the VLAN 1 interface with a VRID of 1:

```
C3(su)->router(Config)#router vrrp
C3(su)->router(Config-router)#create vlan 1 1
```

address

Use this command to configure a virtual router IP address. The **no** form of this command clears the VRRP address configuration.

Syntax

```
address vlan vlan-id vrid ip-address owner
no address vlan vlan-id vrid ip-address owner
```

Parameters

vlan *vlan*-id	Specifies the number of the VLAN on which to configure a virtual router address. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.
vrid	Specifies a unique Virtual Router ID (VRID) associated with the routing interface.
ip-address	Specifies the virtual router IP address to associate with the router.
owner	Specifies a value to indicate if the router owns the IP address as one of its interfaces. Valid values are: • **1** to indicate the router owns the address. • **0** to indicate the router does not own the address.

Defaults

None.

Mode

Router configuration: C3**(su)->router(Config-router)#**

Usage

If the virtual router IP address is the same as the interface (VLAN) address owned by a VRRP router, then the router owning the address becomes the master. The master sends an advertisement to all other VRRP routers declaring its status and assumes responsibility for forwarding packets associated with its virtual router ID (VRID).

If the virtual router IP address is not owned by any of the VRRP routers, then the routers compare their priorities and the higher priority owner becomes the master. If priority values are the same, then the VRRP router with the higher IP address is selected master. For details on using the **priority** command, refer to "priority" on page 20-45.

Example

This example shows how to configure a virtual router address of 182.127.62.1 on the VLAN 1 interface, VRID 1, and to set the router connected to the VLAN via this interface as the master:

```
C3(su)->router(Config)#router vrrp
C3(su)->router(Config-router)#address vlan 1 1 182.127.62.1 1
```

priority

Use this command to set a priority value for a VRRP router. The **no** form of this command clears the VRRP priority configuration.

Syntax

```
priority vlan vlan-id vrid priority-value
no priority vlan vlan-id vrid priority-value
```

Parameters

vlan *vlan*-id	Specifies the number of the VLAN on which to configure VRRP priority. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.
vrid	Specifies a unique Virtual Router ID (VRID) associated with the routing interface. Valid values are from **1** to **255**.
priority-value	Specifies the VRRP priority value to associate with the *vrid*. Valid values are from **1** to **254**, with the highest value setting the highest priority. Priority value of **255** is reserved for the VRRP router that owns the IP address associated with the virtual router. Priority **0** is reserved for signaling that the master has stopped working and the backup router must transition to master state.

Defaults

None.

Mode

Router configuration: C3(su)->router(Config-router)#

Example

This example shows how set a VRRP priority of 200 on the VLAN 1 interface, VRID 1:

```
C3(su)->router(Config)#router vrrp
C3(su)->router(Config-router)#priority vlan 1 1 200
```

advertise-interval

Use this command to set the interval in seconds between VRRP advertisements. The **no** form of this command clears the VRRP advertise interval value.

Syntax

```
advertise-interval vlan vlan-id vrid interval
no advertise-interval vlan vlan-id vrid interval
```

Parameters

vlan *vlan*-id	Specifies the number of the VLAN on which to configure the VRRP advertisement interval. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.
vrid	Specifies a unique Virtual Router ID (VRID) associated with the routing interface. Valid values are from **1** to **255**.
interval	Specifies a VRRP advertisement interval to associate with the *vrid*. Valid values are from **1** to **255** seconds.

Defaults

None.

Mode

Router configuration: C3(su)->router(Config-router)#

Usage

VRRP advertisements are sent by the master router to other routers participating in the VRRP master selection process, informing them of its configured values. Once the master is selected, then advertisements are sent every advertising interval to let other VRRP routers in this VLAN/VRID know the router is still acting as master of the VLAN/VRID.

All routers with the same VRID should be configured with the same advertisement interval.

Example

This example shows how set an advertise interval of 3 seconds on the VLAN 1 interface, VRID 1:

```
C3(su)->router(Config)#router vrrp
C3(su)->router(Config-router)#advertise-interval vlan 1 1 3
```

preempt

Use this command to enable or disable preempt mode on a VRRP router. The **no** form of this command disables preempt mode.

Syntax

preempt *vlan-id vrid*
no preempt *vlan-id vrid*

Parameters

vlan *vlan*-id	Specifies the number of the VLAN on which to set preempt mode. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.
vrid	Specifies a unique Virtual Router ID (VRID) associated with the routing interface. Valid values are from **1** to **255**.

Defaults

None.

Mode

Router configuration: C3(su)->router(Config-router)#

Usage

Preempt is enabled on VRRP routers by default, which allows a higher priority backup router to preempt a lower priority master.

The router that owns the virtual router IP address always preempts other routers, regardless of this setting.

Example

This example shows how to disable preempt mode on the VLAN 1 interface, VRID 1:

```
C3(su)->router(Config)#router vrrp
C3(su)->router(Config-router)#no preempt vlan 1 1
```

enable

Use this command to enable VRRP on an interface. The **no** form of this command disables VRRP on an interface.

Syntax

enable vlan *vlan-id vrid*
no enable vlan *vlan-id vrid*

Parameters

vlan *vlan*-id	Specifies the number of the VLAN on which to enable VRRP. This VLAN must be configured for IP routing as described in "Pre-Routing Configuration Tasks" on page 18-1.
vrid	Specifies the Virtual Router ID (VRID) associated with the *vlan-id*. Valid values are from **1** to **255**.

Defaults

None.

Mode

Router configuration: C3(su)->router(Config-router)#

Example

This example shows how to enable VRRP on the VLAN 1 interface, VRID 1:

```
C3(su)->router(Config)#router vrrp
C3(su)->router(Config-router)#enable vlan 1 1
```

ip vrrp authentication-key

Use this command to enable or disable a VRRP authentication key (password) for use on an interface. The **no** form of this command prevents VRRP from using authentication.

Syntax

ip vrrp authentication-key *name*
no ip vrrp authentication-key

Parameters

name	Specifies the password to enable or disable for VRRP authentication.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the VRRP authentication key chain to "**password"** on the VLAN 1 interface:

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip vrrp authentication-key password
```

show ip vrrp

Use this command to display VRRP routing information.

Syntax

show ip vrrp

Parameters

None.

Defaults

None.

Mode

Any router mode**.**

Example

This example shows how to display VRRP information

```
C3(su)->router(Config)#show ip vrrp

-----------VRRP CONFIGURATION-----------
  Vlan    Vrid    State   Owner  AssocIpAddr  Priority
  2       1     Initialize    0  25.25.2.1      100
```

Configuring PIM-SM

*** Advanced License Required ***

PIM-SM is an advanced routing feature that must be enabled with a license key. If you have purchased an advanced license key, and have enabled routing on the device, you must activate your license as described in the chapter entitled “Activating Licensed Features” in order to enable the PIM-SM command set. If you wish to purchase an advanced routing license, contact Enterasys Networks Sales.

Note: An Enterasys Networks Feature Guide document containing an in-depth discussion of multicast configuration is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

Design Considerations

Enterasys Networks recommends that administrators consider the following recommendations before configuring the SecureStack C3 for a PIM-SM environment.

- A SecureStack C3 **cannot** be configured as a Candidate-RP or a Candidate-BSR.
- A SecureStack C3 **should not** be the first hop router for a multicast stream. In other words, the multicast stream **should not** originate on a SecureStack C3.
- A SecureStack C3 **should not** be positioned in the core of a PIM-SM topology, and **should only** be positioned at the edge in a PIM-SM topology. In other words, the SecureStack C3 **should only** be used to deliver multicast streams to end clients.

Purpose

To enable and configure Protocol Independent Multicast in Sparse Mode (PIM-SM). This protocol provides the means of dynamically learning how to forward multicast traffic in an environment where group members are sparsely located throughout the network and bandwidth is limited. In situations where members are densely located and bandwidth is plentiful, DVMRP would suffice (see “Configuring DVMRP” on page 20-33.)

PIM-SM determines the network topology using the underlying unicast routing protocol to build a Multicast Routing Information Base (MRIB).

Note: IGMP must be enabled on all VLANs running PIM-SM, and must also be globally enabled on the SecureStack C3. For details on enabling IGMP, refer to Chapter 13.

Commands

For information about...	Refer to page...
Global configuration commands	
ip pimsm	20-50
ip pimsm staticrp	20-50
Interface configuration commands	
ip pimsm enable	20-51
ip pimsm query-interval	20-52

ip pimsm

This command sets administrative mode of PIM-SM multicast routing across the router to enabled. IGMP must be enabled before PIM-SM can be enabled. By default, both IGMP and PIM are globally disabled. The **n**o form of this command disables PIM-SM (across the entire stack, if applicable).

Syntax

```
ip pimsm
no ip pimsm
```

Parameters

None.

Defaults

None.

Mode

Global router configuration: C3**(su)->router(Config)#**

Example

This example shows how to globally enable and disable PIM:

```
C3(su)->router(Config)# ip pimsm
C3(su)->router(Config)# no ip pimsm
```

ip pimsm staticrp

This command is used to create a manual Rendezvous Point IP address for the PIM-SM router. The **no** form of this command removes a previously configured RP.

Syntax

```
ip pimsm staticrp ipaddress groupadress groupmask
no ip pimsm staticrp ipaddress groupadress groupmask
```

Parameters

ipaddress	The IP address of the Rendezvous Point
groupadress	The group address supported by the Rendezvous Point
groupmask	The group mask for the group address

Defaults

None.

Mode

Global Router configuration: C3**(su)->router(Config)#**

Example

This example shows how to set an RP for a specific multicast group.

```
C3(su)->router(Config)# ip pimsm staticrp 192.15.18.3 224.0.0.0 240.0.0.0
```

ip pimsm enable

This command sets the administrative mode of PIM-SM multicast routing on a routing interface to enabled. By default, PIM is disabled on all IP interfaces. The **no** form of this command disables PIM on the specific interface.

Syntax

```
ip pimsm enable
no ip pimsm enable
```

Parameters

None.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to enable PIM on IP interface for VLAN 1.

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip pimsm enable
```

ip pimsm query-interval

This command configures the transmission frequency of hello messages in seconds between PIM-enabled neighbors. The **no** form of this command resets the hello interval to the default, 30 seconds.

Syntax

ip pimsm query-interval *seconds*

no ip pimsm query-interval

Parameters

seconds	This field has a range of **10** to **3600** seconds. Default is **30**.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan 1))#

Example

This example shows how to set the hello interval rate to 100 seconds.

```
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip pimsm query-interval 100
```

show ip pimsm

Use this command to display system-wide PIM-SM routing information.

Syntax

show ip pimsm

Parameters

None.

Defaults

None.

Mode

Any router mode**.**

Example

This example shows how to display PIM information.

```
C3(su)->router# show ip pimsm

Admin Mode Enable
Join/Prune Interval (secs) 60
```

```
PIM-SM INTERFACE STATUS
 VlanId    Interface Mode  Protocol State
---------  --------------  ---------------
8          Disable         Non-Operational
16         Enable          Operational
17         Enable          Operational
20         Enable          Operational
30         Enable          Operational
31         Disable         Non-Operational
32         Disable         Non-Operational
33         Disable         Non-Operational
```

Table 20-7 provides an explanation of the command output.

Table 20-7 show ip pimsm Output Details

Output Field	What it displays
Admin Mode	This field indicates whether PIM-SM is enabled or disabled. This is a configured value.
Join/Prune Interval (secs)	This field shows the interval at which periodic PIM-SM Join/Prune messages are to be sent.
VlanId	VLAN id associated with the PIM IP Interface.
Interface Mode	This field indicates whether PIM-SM is enabled or disabled on the interface. This is a configured value.
Protocol State	This field indicates the current state of the PIM-SM protocol on the interface. Possible values are Operational or Non-Operational.

show ip pimsm componenttable

This command displays the table containing objects specific to a PIM domain. One row exists for each domain to which the router is connected.

Syntax

show ip pimsm componenttable

Parameters

None.

Defaults

None.

Mode

Any router mode.

Example

This example shows how to display PIM router information:

```
C3(su)->router> show ip pimsm componenttable
```

```
                    COMPONENT TABLE

Component   Component       Component       Component
Index       BSR Address     BSR Expiry Time CRP Hold Time
                            (hh:mm:ss)      (hh:mm:ss)
----------  --------------- --------------- -------------
1            192.168.30.2    00:02:10        00:00:00
```

Table 20-8 provides an explanation of the command output.

Table 20-8 show ip pimsm componenettable Output Details

Output Field	What it displays
Component Index	This field displays a number which uniquely identifies the component.
Component BSR Address	This field displays the IP address of the bootstrap router (BSR) for the local PIM region.
Component BSR Expiry Time	This field displays the minimum time remaining before the BSR in the local domain will be declared down.
Component CRP Hold Time	This field displays the hold time of the component when it is a candidate rendezvous point.

show ip pimsm interface

This command displays PIM-SM status of the router interfaces. With the **stats** parameter, this command displays statistical information for PIM-SM on the specified interface.

Syntax

show ip pimsm interface {**vlan** *vlan-id* | **stats** {*vlan-id* | **all**}}

Parameters

vlan *vlan-id*	Display PIM-SM information for the specified IP interface enabled for PIM.
stats	Display PIM-SM interface statistics.
vlan-id | **all**	Display statistics for a specific VLAN or all VLANs.

Defaults

None.

Mode

Any router mode.

Examples

This example shows how to display PIM interface information.

```
C3(su)->router> show ip pimsm interface vlan 30

VLAN ID                       30
IP Address                    192.168.30.1
Subnet Mask                   255.255.255.0
Mode                          enable
```

```
Hello Interval (secs)         30 secs
CBSR Preference               -1
CRP Preference                -1
CBSR Hash Mask Length         30
```

Table 20-9 provides an explanation of the **show ip pimsm interface vlan** command output.

Table 20-9 show ip pimsm interface vlan Output Details

Output Field	What it displays
IP Address	The IP address of the specified interface.
Subnet Mask	The Subnet Mask for the IP address of the PIM interface.
Mode	Indicates whether PIM-SM is enabled or disabled on the specified interface. This is a configured value. By default it is disabled.
Hello Interval	Indicates the frequency at which PIM hello messages are transmitted on this interface. This is a configured value. By default, the value is 30 seconds
CBSR Preference	The preference value for the local interface as a candidate bootstrap router.
CRP Preference	The preference value as a candidate rendezvous point on this interface.
CBSR Hash Mask Length	The hash mask length to be advertised in bootstrap messages if this interface is elected as the bootstrap router. The value is used in the hash algorithm for selecting the RP for a particular group.

This example shows how to display PIM interface statistics.

```
C3(su)->router> show ip pimsm interface stats all
                                                                  Neighbor
Vlan ID     IP Address       Subnet Mask      Designated Router  count
---------  ---------------  ---------------  -----------------  ----------
6          192.168.6.2       255.255.255.0     0.0.0.0              0
7          192.168.7.1       255.255.255.0     192.168.7.1          0
8          192.168.8.1       255.255.255.0     0.0.0.0              0
30         192.168.30.1      255.255.255.0     192.168.30.2         1
```

Table 20-10 provides an explanation of the **show ip pimsm interface stats** command output.

Table 20-10 show ip pimsm interface stats Output Details

Output Field	What it displays
IP Address	The IP Address that represents the PIM-SM interface.
Subnet Mask	The Subnet Mask of this PIM-SM interface.
Designated Router	IP Address of the Designated Router for this interface.
Neighbor Count	The number of neighbors on the PIM-SM interface.

show ip pimsm neighbor

Display the router's PIM neighbors.

Syntax

show ip pimsm neighbor [*vlan-id*]

Parameters

vlan-id	(Optional) Display all neighbors discovered on a specific Interface.

Mode

Any router mode.

Defaults

If the VLAN id is omitted, all neighbors off all interfaces will be displayed.

Example

This example shows how to display PIM information:

```
C3(su)->router> show ip pimsm neighbor

                    NEIGHBOR TABLE
Vlan ID    IP Address         Up Time     Expiry Time
                              (hh:mm:ss)  (hh:mm:ss)
---------  ----------------   ----------  ------------
30         192.168.30.2       01:36:41     00:01:25
6          192.168.6.1        01:36:41     00:01:25
```

Table 20-11 provides an explanation of the command output.

Table 20-11 show ip pimsm neighbor Output Details

Output Field	What it displays
Vlan ID	VLAN id of the interface.
IP Address	The IP Address of the neighbor on an interface
Up Time	The time since this neighbor has become active on this interface.
Expiry Time	The expiry time of the neighbor on this interface.

show ip pimsm rp

This command displays the PIM information for candidate Rendezvous Points (RPs) for all IP multicast groups or for a specific group address. The information in the table is displayed for each IP multicast group.

Syntax

show ip pimsm rp {*group-address group-mask* | **all** | **candidate**}

Parameters

group-address	The multicast group IP address.
group-mask	The multicast group address subnet mask.
all	For all known group addresses.
candidate	Display PIM-SM candidate-RP table information.

Defaults

None.

Mode

Any router mode.

Examples

This example shows how to display the RP set for a specific group address.

```
C3(su)->router> show ip pimsm rp 224.0.0.0 240.0.0.0

                                    RP SET TABLE
Group
Address    Group Mask   Address      Hold Time   Expiry Time Component C-RP Priority
                                     (hh:mm:ss)  (hh:mm:ss)
---------  ----------  -----------  ---------- ----------- --------- -----------
224.0.0.0 240.0.0.0   192.168.30.2  00:02:15    00:02:30     1         0
```

Table 20-12 provides an explanation of the command output.

Table 20-12 show ip pimsm rp Output Details

Output Field	What it displays
Group Address	The address of the group for which the RP set is displayed.
Group Mask	The mask of the group address.
Address	The IP address of the RP.
Hold Time	The hold time of the RP.
Expiry Time	The minimum time remaining before the RP will be declared down.
Component	A number which uniquely identifies the component. Each protocol instance connected to a separate domain should have a different index value.
C-RP Priority	The candidate-RP priority of the RP.

This example shows how to display the candidate RPs for each group address.

```
C3(su)->router> show ip pimsm rp candidate

             CANDIDATE RP TABLE
Group Address    Group Mask      Address
---------------- --------------- ---------------
224.0.0.0        240.0.0.0       192.168.30.2
```

show ip pimsm rphash

Displays the Rendezvous Point router that will be selected from the set of active RP routers. The RP router, for the group, is selected by using the hash algorithm defined in RFC 2362.

Syntax

show ip pimsm rphash *group-address*

Parameters

group-address	The Group Address for the RP.

Defaults

None.

Mode

Any router mode.

Example

This example shows how to display RP that will be selected for group address 224.0.0.0:

```
C3(su)->router> show ip pimsm rphash 224.0.0.0
192.168.129.223
```

show ip pimsm staticrp

Display the PIM-SM static Rendezvous Point information.

Syntax

show ip pimsm staticrp

Parameters

None.

Mode

Any router mode.

Defaults

None.

Example

This example shows how to display PIM information.

```
C3(su)->router# show ip pimsm staticrp

             STATIC RP TABLE
    Address      Group Address    Group Mask
--------------- --------------- ---------------
123.231.111.121 234.0.0.0       255.0.0.0
192.168.129.223 224.0.0.0       240.0.0.0
```

Table 20-13 provides an explanation of the command output.

Table 20-13 show ip pimsm staticrp Output Details

Output Field	What it displays
Address	The IP address of the RP.
Group Address	The group address supported by the RP.
Group Mask	The group mask for the group address.

show ip mroute

Use this command to display the IP multicast routing table.

Syntax

```
show ip mroute
```

Parameters

None.

Defaults

None.

Mode

Any router mode.

Usage

The multicast routing table shows how a multicast routing protocol, such as PIM and DVMRP, will forward a multicast packet. Information in the table includes source network/mask and upstream neighbors.

For information about DVMRP, see "Configuring DVMRP" on page 20-33.

Example

This example shows the output of this command.

```
C3(su)->router#show ip mroute
Active IP Multicast Sources
Flags: D - Dense, S - Sparse, C - Connected, L - Local,P - Pruned, R - RP-bit set,
F - Register flag, T - SPT-bit set,Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

Source Network   : 192.168.111.10
Source Mask      : 0.0.0.0
MultiCast Group  : 239.1.8.9
Uptime           : 6336
Upstream Neighbor: 0.0.0.0
Upstream Vlan    : 111
Downstream Vlans : 8

Source Network   : 192.168.111.10
Source Mask      : 0.0.0.0
MultiCast Group  : 239.1.7.105
Uptime           : 6336
```

```
Upstream Neighbor: 0.0.0.0
Upstream Vlan    : 111
Downstream Vlans : 8

Source Network   : 192.168.111.10
Source Mask      : 0.0.0.0
MultiCast Group  : 239.1.8.169
Uptime           : 6582
Upstream Neighbor: 0.0.0.0
Upstream Vlan    : 111
Downstream Vlans : 8

Source Network   : 192.168.111.10
Source Mask      : 0.0.0.0
MultiCast Group  : 239.1.4.173
Uptime           : 6582
Upstream Neighbor: 0.0.0.0
Upstream Vlan    : 111
Downstream Vlans : 8
```

21

IPv6 Management

This chapter describes the switch mode set of commands used to manage IPv6.

Purpose

To enable or disable the IPv6 management function, to configure and display the IPv6 host address and IPv6 gateway for the switch, and to display IPv6 status information.

Commands

show ipv6 status

Use this command to display the status of the IPv6 management function.

Syntax

```
show ipv6 status
```

Parameters

None.

Defaults

None.

Mode

Switch mode, read-only.

Example

This example shows how to display IPv6 management function status.

```
C3(ro)->show ipv6 status
IPv6 Administrative Mode: Disabled
```

set ipv6

Use this command to globally enable or disable the IPv6 management function.

Syntax

set ipv6 {**enable** | **disable**}

Parameters

enable | **disable**	Enable or disable the IPv6 management function.

Defaults

By default, IPv6 management is disabled.

Mode

Switch mode, read-write.

Usage

When you enable IPv6 management on the switch, the system automatically generates a link-local host address for the switch from the host MAC address. You can set a different host IPv6 address with the **set ipv6 address** command.

Example

This example shows how to enable IPv6 management.

```
C3(su)-> set ipv6 enable

C3(su)->show ipv6 status
IPv6 Administrative Mode: Enabled

C3(su)->show ipv6 address
Name            IPv6 Address
------------    ----------------------------------------
host            FE80::201:F4FF:FE5C:2880/64
```

set ipv6 address

Use this command to configure IPv6 global addressing information.

Syntax

set ipv6 address *ipv6-addr/prefix-length* [**eui64**]

Parameters

ipv6-addr	The IPv6 address or prefix to be configured. This parameter must be in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
prefix-length	The length of the IPv6 prefix for this address. The value of *prefix-length* is a decimal number indicating the number of high-order contiguous bits of the address that comprise the network portion of the address.
eui64	(Optional) Formulate the IPv6 address using an EUI-64 ID in the lower order 64 bits of the address.

Defaults

No global unicast IPv6 address is defined by default.

Mode

Switch mode, read-write.

Usage

Use this command to manually configure a global unicast IPv6 address for IPv6 management. You can specify the address completely, or you can use the optional **eui64** parameter to allow the switch to generate the lower order 64 bits of the address.

When using the **eui64** parameter, you specify only the network prefix and length.

Examples

This example shows how to completely specify an IPv6 address by entering all 128 bits and the prefix:

```
C3(su)->set ipv6 address 2001:0db8:1234:5555::9876:2/64

C3(su)->show ipv6 address
Name            IPv6 Address
------------    ----------------------------------------
host            FE80::201:F4FF:FE5C:2880/64
host            2001:DB8:1234:5555::9876:2/64
```

This example shows how to use the **eui64** parameter to configure the lower order 64 bits:

```
C3(su)->set ipv6 address 2001:0db8:1234:5555::/64 eui64

C3(su)->show ipv6 address
Name            IPv6 Address
------------    ----------------------------------------
host            FE80::201:F4FF:FE5C:2880/64
host            2001:DB8:1234:5555:201:F4FF:FE5C:2880/64
```

show ipv6 address

Use this command to display the system IPv6 address(es) and IPv6 gateway address (default router), if configured.

Syntax

show ipv6 address

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Usage

This command displays the IPv6 addresses configured automatically and with the **set ipv6 address** and **set ipv6 gateway** commands.

Example

This example displays three IPv6 management addresses configured for the switch.

```
C3(su)->show ipv6 address
Name            IPv6 Address
------------    ---------------------------------------
host            FE80::201:F4FF:FE5C:2880/64
host            2001:DB8:1234:5555:201:F4FF:FE5C:2880/64
gateway         FE80::201:F4FF:FE5D:1234
```

clear ipv6 address

Use this command to clear IPv6 global addresses.

Syntax

clear ipv6 [**address** {**all**|*ipv6-addr/prefix-length*}]

Parameters

ipv6-addr	The IPv6 address to be cleared. This parameter must be in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
prefix-length	The length of the IPv6 prefix for this address. The value of *prefix-length* is a decimal number indicating the number of high-order contiguous bits of the address that comprise the network portion of the address.
all	Deletes all IPv6 global addresses.

Defaults

If **address** is not entered, all manually configured global IPv6 addresses are cleared.

Mode

Switch mode, read-write.

Usage

This command clears addresses manually configured with the **set ipv6 address** command. Use the **clear ipv6 gateway** command to clear the IPv6 gateway address.

Example

This example illustrates that this command clears only those IPv6 addresses configured with the **set ipv6 address** command. The link-local address for the host interface and the gateway address are not removed with this command.

```
C3(su)->show ipv6 address
Name            IPv6 Address
------------    ----------------------------------------
host            FE80::201:F4FF:FE5C:2880/64
host            2001:DB8:1234:5555:201:F4FF:FE5C:2880/64
host            2001:DB8:1234:5555::9876:2/64
gateway         FE80::201:F4FF:FE5D:1234

C3(su)->clear ipv6 address all

C3(su)->show ipv6 address
Name            IPv6 Address
------------    ----------------------------------------
host            FE80::201:F4FF:FE5C:2880/64
gateway         FE80::201:F4FF:FE5D:1234
```

set ipv6 gateway

Use this command to configure the IPv6 gateway (default router) address.

Syntax

set ipv6 gateway *ipv6-addr*

Parameters

ipv6-addr	The IPv6 address to be configured. The address can be a global unicast or link-local IPv6 address, in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.

Defaults

None.

Mode

Switch mode, read-write.

Usage

This command configures the IPv6 gateway address. Only one IPv6 gateway address can be configured for the switch, so executing this command when a gateway address has already been configured will overwrite the previously configured address.

Use the **show ipv6 address** command to display a configured IPv6 gateway address.

Example

This example shows how to configure an IPv6 gateway address using a link-local address.

```
C3(su)->set ipv6 gateway fe80::201:f4ff:fe5d:1234
C3(su)->show ipv6 address
Name            IPv6 Address
------------    ---------------------------------------
host            FE80::201:F4FF:FE5C:2880/64
gateway         FE80::201:F4FF:FE5D:1234
```

clear ipv6 gateway

Use this command to clear an IPv6 gateway address.

Syntax

clear ipv6 gateway

Parameters

None.

Defaults

None.

Mode

Switch mode, read-write.

Example

This example shows how to remove a configured IPv6 gateway address.

```
C3(su)->show ipv6 address
Name            IPv6 Address
------------    ---------------------------------------
host            FE80::201:F4FF:FE5C:2880/64
gateway         FE80::201:F4FF:FE5D:1234

C3(su)->clear ipv6 gateway

C3(su)->show ipv6 address
Name            IPv6 Address
------------    ---------------------------------------
host            FE80::201:F4FF:FE5C:2880/64
```

show ipv6 neighbors

Use this command to display the system IPv6 Neighbor Discovery Protocol cache.

Syntax

show ipv6 neighbors

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows example output of this command.

```
C3(su)->show ipv6 neighbors
                                                                                Last
IPv6 Address                              MAC Address       isRtr State     Updated
----------------------------------------- ----------------- ----- -------   -------
2001:db8:1234:6666::2310:3            00:04:76:73:42:31 True  Reachable 00:01:16
```

show ipv6 netstat

Use this command to display IPv6 netstat information.

Syntax

show ipv6 netstat

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows the output of this command.

```
C3(su)->show ipv6 netstat
Prot Local   Address                                 State
     Foreign Address
---- ---------------------------------------------- -----------
TCP  3333::211:88FF:FE59:4424.22                    ESTABLISHED
     2020::D480:1384:F58C:B114.1049
TCP  3333::211:88FF:FE59:4424.443                   TIME_WAIT
     2020::D480:1384:F58C:B114.1056
TCP  ::.23                                          LISTEN
     ::.*
TCP  3333::211:88FF:FE59:4424.22                    ESTABLISHED
     2020::D480:1384:F58C:B114.1050
TCP  3333::211:88FF:FE59:4424.22                    ESTABLISHED
     3333::2117:F1C0:90B:910D.1045
TCP  ::.80                                          LISTEN
```

```
     ::.*
TCP  ::.22                                          LISTEN
     ::.*

TCP  3333::211:88FF:FE59:4424.80                    ESTABLISHED
     2020::D480:1384:F58C:B114.1053
TCP  3333::211:88FF:FE59:4424.80                    ESTABLISHED
     2020::D480:1384:F58C:B114.1054
TCP  ::.443                                         LISTEN
     ::.*
TCP  3333::211:88FF:FE59:4424.22                    ESTABLISHED
     2020::D480:1384:F58C:B114.1048
TCP  3333::211:88FF:FE59:4424.443                   TIME_WAIT
     2020::D480:1384:F58C:B114.1055
```

ping ipv6

Use this command to test routing network connectivity by sending IP ping requests.

Syntax

ping *ipv6-addr* [**size** *num*]

Parameters

ipv6-addr	Specifies the IPv6 address of the system to ping. Enter the address in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
size *num*	(Optional) Specifies the size of the datagram packet. The value of *num* can range from 48 to 2048 bytes.

Defaults

None.

Mode

Switch mode, read-write.

Usage

This command is also available in router mode.

Examples

This example shows output from a successful ping to IPv6 address 2001:0db8:1234:5555::1234:1.

```
C3(su)->ping ipv6 2001:0db8:1234:5555::1234:1
 2001:DB8:1234:5555::1234:1 is alive
```

This example shows output from an unsuccessful ping to IPv6 address 2001:0db8:1234:5555::1234:1.

```
C3(su)->ping ipv6 2001:0db8:1234:5555::1234:1
 no answer from 2001:DB8:1234:5555::1234:1
```

traceroute ipv6

Use this command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis.

Syntax

traceroute ipv6 *ipv6-addr*

Parameters

ipv6-addr	Specifies a host to which the route of an IPv6 packet will be traced. Enter the address in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.

Defaults

None.

Mode

Switch mode, read-write.

Usage

This command is also available in router mode.

Example

This example shows how to use traceroute to display a round trip path to host `2001:0db8:1234:5555`

```
C3(su)->router#traceroute ipv6 2001:0db8:1234:5555::1
Traceroute to 2001:0db8:1234:5555, 30 hops max, 40 byte packets
 1 2001:0db8:1234:5555        1.000000e+00 ms   1.000000e+00 ms   1.000000e+00 ms
```

22

IPv6 Configuration

*** IPv6 Routing License Required ***

IPv6 routing must be enabled with a license key. If you have purchased an IPv6 routing license key, and have enabled routing on the device, you must activate your license as described in the chapter entitled "Activating Licensed Features" in order to enable the IPv6 routing configuration command set. If you wish to purchase an IPv6 routing license, contact Enterasys Networks Sales.

The commands in this chapter perform configuration of IPv6 parameters on the SecureStack C3. For information about specific IPv6 routing protocols, such as OSFPv3, refer to the appropriate chapters. For information about managing IPv6 functionality at the switch level, refer to Chapter 21, **IPv6 Management**.

Overview

IPv6 and IPv4 coexist on the SecureStack C3. As with IPv4, IPv6 routing can be enabled on VLAN interfaces. Each Layer 3 routing interface can be used for IPv4, IPv6, or both.

The SecureStack C3 supports all IPv6 address formats, including global unicast addresses, link-local unicast, global multicast, scoped multicast (including local scoped multicast), IPv4 compatible addresses, unspecified addresses, loopback addresses, and anycast addresses.

Refer to the following RFCs for more information about IPv6 address formats:

- RFC 4291, "IP Version 6 Addressing Architecture"
- RFC 3587, "IPv6 Global Unicast Address Format"
- RFC 4007, "IPv6 Scoped Address Architecture"

The basic IPv6 protocol specifies PDU options of two classes, both of which are supported: hop-by-hop options and destination options. While new options can be defined in the future, the following are currently supported: routing (for source routing), fragment, router alert and pad. Jumbograms are not supported. In IPv6, only source nodes fragment. Path MTU discovery is therefore a requirement. Flow labels are ignored.

Neighbor Discovery is the IPv6 replacement for ARP. The SecureStack C3 supports neighbor advertise and solicit, duplicate address detection, and unreachability detection. Router Advertisement is part of the Neighbor Discovery process and is required for IPv6. Stateless

autoconfiguration is part of Router Advertisement and the SecureStack C3 can support both stateless and stateful autoconfiguration of end nodes. The SecureStack C3 supports both EUI-64 interface identifiers and manually configured interface IDs.

Refer to the following RFCs for more information about Neighbor Discovery and stateless address autoconfiguration:

- RFC 2461, "Neighbor Discovery for IP Version 6"
- RFC 2462, "IPv6 Stateless Address Autoconfiguration"

For ICMPv6, error PDU generation is supported, as are path MTU, echo, and redirect.

Router Advertisement is an integral part of IPv6 and is supported. Numerous options are available including stateless/stateful address configuration, router and address lifetimes, and Neighbor Discovery timer control. Ping and traceroute applications for IPv6 are provided.

Management of IPv6 features is provided by means of CLI commands and SNMP. See Chapter 21, **IPv6 Management** for descriptions of the CLI commands.

Default Conditions

The following table lists the default IPv6 conditions.

Condition	Default Value
IPv6 forwarding	Enabled
IPv6 route distance	1
IPv6 unicast-routing	Disabled
IPv6 enable	Disabled
IPv6 mtu	1500
IPv6 nd dad attempts	1
IPv6 nd managed-config-flag	False
IPv6 nd ns-interval	0
IPv6 nd other-config-flag	False
IPv6 nd ra-interval	600
IPv6 nd ra-lifetime	1800
IPv6 nd reachable-time	0
IPv6 nd suppress-ra	Disabled
IPv6 nd prefix	Valid-lifetime — 604800 Preferred-lifetime — 2592000 Autoconfig — enabled On-link — enabled

General Configuration Commands

ipv6 forwarding

This command enables or disables IPv6 forwarding on the router.

Syntax

```
ipv6 forwarding
no ipv6 forwarding
```

Parameters

None.

Defaults

IPv6 forwarding is enabled.

Mode

Router global configuration: C3(su)->router(Config)#

Usage

The **no** form of this command disables IPv6 forwarding on the router.

Example

This example disables IPv6 forwarding.

```
C3(su)->router(Config)# no ipv6 forwarding
```

ipv6 hop-limit

This command sets the maximum number of IPv6 hops used in IPv6 packets and router advertisements generated by this device.

Syntax

```
ipv6 hop-limit hops
no ipv6 hop-limit
```

Parameters

hops	Specifies the maximum number of IPv6 hops used in IPv6 packets and router advertisements generated by this device. Value can range from 1 to 255. The default value is 64.

Defaults

The default maximum number of IPv6 hops is 64.

Mode

Router global configuration: C3(su)->router(Config)#

Usage

This command sets the value of the hop limit field in IPv6 packets originated by this device. This value is also placed in the "Cur Hop Limit" field of router advertisements generated by this router.

Use the **no** form of this command to reset the limit to the default value.

Example

This example sets the hop limit to 50.

```
C3(su)->router(Config)# ipv6 hop-limit 50
```

ipv6 route

This command configures static IPv6 routes.

Syntax

ipv6 route *ipv6-prefix/prefix-length* **interface** {**tunnel** *tunnel-id* | **vlan** *vlan-id*} *next-hop-addr* [*pref*]
no ipv6 route *ipv6-prefix/prefix-length* **interface** {**tunnel** *tunnel-id* | **vlan** *vlan-id*} *next-hop-addr* [*pref*]

Parameters

ipv6-prefix/prefix-length	The IPv6 network prefix that is the destination of the static route, and the prefix length. The prefix must be in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons. The prefix length is a decimal number indicating the number of high-order contiguous bits of the address that comprise the network portion of the address.
interface tunnel *tunnel-id* | **vlan** *vlan-id*	Specifies the interface type and ID of direct static routes from point-to-point and broadcast interfaces.

next-hop-addr	Link-local address of the interface.
pref	(Optional) Specifies the preference value the router uses to compare this route with routes from other route sources that have the same destination. The value of *pref* can range from1 to 255. The default value is 1, which gives static routes precedence over any other type of route except connected routes. A route with a preference of 255 cannot be used to forward traffic.

Defaults

Default preference or administrative distance is 1.

Mode

Router global configuration: C3(su)->router(Config)#

Usage

Use the **no** form of this command to remove a static route. If you do not specify a next hop address with the **no** form, all static routes to the specified destination will be removed.

Example

This command creates a static IPv6 route to network 2001:0DB8:2222:4455::/64 by way of interface VLAN 6 and gives it a preference of 5.

```
C3(su)->router(Config)# ipv6 route 2001:0DB8:2222:4455::/64 interface vlan 6
fe80::1234:5678:2dd:1 5
```

ipv6 route distance

This command configures the default distance, or preference, for static IPv6 routes.

Syntax

ipv6 route distance *pref*
no ipv6 route distance

Parameters

pref	A distance value used when no distance is specified when a static route is configured. The value can range from 1 to 255. Lower route distance values are preferred when determining the best route.

Defaults

Default preference or administrative distance is 1.

Mode

Router global configuration: C3(su)->router(Config)#

Usage

The default distance is used when no distance is specified in the **ipv6 route** command. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the **ipv6 route distance** command.

Use the **no** form of this command to return the default distance to 1.

Example

This command sets the default distance value to 3.

```
C3(su)->router(Config)# ipv6 route distance 3
```

ipv6 unicast-routing

This command enables/disables forwarding of IPv6 unicast datagrams.

Syntax

ipv6 unicast-routing

no ipv6 unicast-routing

Parameters

None.

Defaults

Disabled.

Mode

Router global configuration: C3(su)->router(Config)#

Usage

Use this command to enable forwarding of IPv6 unicast datagrams on the SecureStack C3. Use the **no** form of the command to disable forwarding of IPv6 unicast datagrams.

Example

This command enables forwarding of IPv6 unicast datagrams on the router.

```
C3(su)->router(Config)# ipv6 unicast-routing
```

ping ipv6

Use this command to test routing network connectivity by sending IP ping requests.

Syntax

ping ipv6 *ipv6-addr* [**size** *num*]

Parameters

ipv6-addr	Specifies the global IPv6 address of the system to ping. Enter the address in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
size *num*	(Optional) Specifies the size of the datagram packet. The value of *num* can range from 48 to 2048 bytes.

Defaults

None.

Mode

Router privileged exec: C3(su)->router#

Router user exec: C3(su)->router>

Usage

Use this command to determine whether another computer is on the network. To use this command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP.

The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station.

Examples

This example shows output from a successful ping to IPv6 address 2001:0db8:1234:5555::1234:1.

```
C3(su)->router#ping ipv6 2001:0db8:1234:5555::1234:1
Send count=3, Receive count=3 from 2001:DB8:1234:5555::1234:1
Average round trip time = 1.00 ms
```

This example shows output from an unsuccessful ping to IPv6 address 2001:0db8:1234:5555::1234:1.

```
C3(su)->ping ipv6 2001:0db8:1234:5555::1234:1
 no answer from 2001:DB8:1234:5555::1234:1
```

ping ipv6 interface

Use this command to test routing network connectivity by sending IP ping requests.

Syntax

ping ipv6 interface {**vlan** *vlan-id* | **tunnel** *tunnel-id* | **loopback** *loop-id*} {**link-local-address** *ipv6-lladdr* | *ipv6-addr*} [**size** *num*]

Parameters

vlan *vlan-id*	Specifies a VLAN interface as the source.
tunnel *tunnel-id*	Specifies a tunnel interface as the source.
loopback *loop-id*	Specifies a loopback interface as the source.
link-local-address *ipv6-lladdr*	Specifies a link-local IPv6 address to ping.

ipv6-addr	Specifies the global IPv6 address of the system to ping. Enter the address in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
size *num*	(Optional) Specifies the size of the datagram packet. The value of *num* can range from 48 to 2048 bytes.

Defaults

None.

Mode

Router privileged exec: C3(su)->router#

Usage

Use this command to ping an interface by using the link-local address or the global IPv6 address of the interface. You can use a loopback, tunnel, or logical interface as the source. The source and target devices must have the ping utility enabled and running on top of TCP/IP.

The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station.

Example

This example shows output from a successful ping to link-local address fe80::211:88ff:fe55:4a7f.

```
C3(su)->router#ping ipv6 interface vlan 6 link-local-address
fe80::211:88ff:fe55:4a7f
Send count=3, Receive count=3 from fe80::211:88ff:fe55:4a7f
Average round trip time = 1.00 ms
```

traceroute ipv6

Use this command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis.

Syntax

traceroute ipv6 *ipv6-addr*

Parameters

ipv6-addr	Specifies a host to which the route of an IPv6 packet will be traced. Enter the address in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.

Defaults

None.

Mode

Router privileged exec: C3 (su)->router#

Example

This example shows how to use traceroute to display a round trip path to host 2001:0db8:1234:5555::1.

```
C3(su)->router#traceroute ipv6 2001:0db8:1234:5555::1
Traceroute to 2001:0db8:1234:5555::1, 30 hops max, 40 byte packets
 1 2001:0db8:1234:5555::1      1.000000e+00 ms  1.000000e+00 ms  1.000000e+00 ms
```

Interface Configuration Commands

ipv6 address

This command configures a global IPv6 address on an interface, including VLAN, tunnel, and loopback interfaces, and enables IPv6 processing on the interface.

Syntax

ipv6 address {*ipv6-addr/prefix-length* | *ipv6-prefix/prefix-length* **eui64**}
no ipv6 address [*ipv6-addr/prefix-length* | *ipv6-prefix/prefix-length* **eui64**]

Parameters

ipv6-addr	The IPv6 address to be configured on the interface. This parameter must be in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
prefix-length	The length of the IPv6 prefix for this address. The value of *prefix-length* is a decimal number indicating the number of high-order contiguous bits of the address that comprise the network portion of the address. If the **eui64** parameter is used, this value must be 64 bits.
ipv6-prefix	The IPv6 prefix to be configured on the interface. This parameter must be in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.
eui64	Configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits of the address and enables IPv6 processing on the interface.

Defaults

No IPv6 addresses are defined for any interface.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

Use this command to manually configure a global IPv6 address on an interface. You can enter the complete 128-bit address and prefix, or use the **eui64** parameter to configure a global IPv6 address using an EUI-64 identifier in the low order 64 bits of the address. When using the **eui64** parameter, you specify only the network prefix and length, and the SecureStack C3 generates the low order 64 bits.

The hexadecimal letters in the IPv6 addresses are not case-sensitive.

This command also enables IPv6 processing on the interface and automatically generates a link-local address.

You can assign multiple globally reachable addresses to an interface with this command.

Use the **no ipv6 address** command without any parameters to remove all manually configured IPv6 addresses from the interface.

Example

This example configures an IPv6 address by using the **eui64** parameter. Then, the **show ipv6 interface** is executed to display the configuration. Note that a link-local address has also automatically been generated.

```
C3(su)->router(Config-if(Vlan 7))# ipv6 address 3FFE:501:FFFF:101/64 eui64
C3(su)->router>show ipv6 interface vlan 7

Vlan 7 Administrative Mode                      Enabled
Vlan 7 IPv6 Routing Operational Mode            Enabled
IPv6 is                                         Enabled
IPv6 Prefix is                                  FE80::211:88FF:FE55:4A7F/128
                                      3FFE:501:FFFF:101:211:88FF:FE55:4A7F/64
Routing Mode                                    Enabled
Interface Maximum Transmit Unit                 1500
Router Duplicate Address Detection Transmits    1
Router Advertisement NS Interval                0
Router Lifetime Interval                        1800
Router Advertisement Reachable Time             0
Router Advertisement Interval                   600
Router Advertisement Managed Config Flag        Disabled
Router Advertisement Other Config Flag          Disabled
Router Advertisement Suppress Flag              Disabled
```

ipv6 enable

This command enables IPv6 routing on an interface that has not been configured with an explicit IPv6 address.

Syntax

```
ipv6 enable
no ipv6 enable
```

Parameters

None.

Defaults

IPv6 is disabled.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

When this command is executed, an IPv6 link-local unicast address is configured on the interface and IPv6 processing is enabled. You do not need to use this command if you configured an IPv6 global address on an interface with the **ipv6 address** command.

The **no ipv6 enable** command disables IPv6 routing on an interface that has been enabled with the **ipv6 enable** command, but it does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Example

This example enables IPv6 processing on VLAN 7. Note that a link-local address has been automatically configured.

```
C3(su)->router(Config-if(Vlan 7))# ipv6 enable
C3(su)->router>show ipv6 interface vlan 7

Vlan 7 Administrative Mode                        Enabled
Vlan 7 IPv6 Routing Operational Mode              Enabled
IPv6 is                                           Enabled
IPv6 Prefix is                                    FE80::211:88FF:FE55:4A7F/128
Routing Mode                                      Enabled
Interface Maximum Transmit Unit                   1500
Router Duplicate Address Detection Transmits      1
Router Advertisement NS Interval                  0
Router Lifetime Interval                          1800
Router Advertisement Reachable Time               0
Router Advertisement Interval                     600
Router Advertisement Managed Config Flag          Disabled
Router Advertisement Other Config Flag            Disabled
Router Advertisement Suppress Flag                Disabled
```

ipv6 mtu

This command configures the maximum transmission unit (MTU) size of IPv6 packets that can be sent on an interface.

Syntax

ipv6 mtu *bytes*
no ipv6 mtu

Parameters

bytes	Specifies the MTU value in bytes. The value can range from 1280 to 1500 bytes. The MTU cannot be larger than the value supported by the underlying interface.

Defaults

1480 bytes

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

The maximum transmission unit is the largest possible unit of data that can be sent on a given physical medium. Use this command to set the MTU for an IPv6 interface. The **no** form of this command resets the MTU to the default value of 1480 bytes.

Use the show ipv6 interface to display the current setting for this interface.

Note: All interfaces attached to the same physical medium must be configured with the same MTU to operate properly.

Example

This example sets the MTU value to 1500 bytes.

```
C3(su)->router(Config-if(Vlan 1))# ipv6 mtu 1500
```

Neighbor Cache and Neighbor Discovery Commands

The IPv6 Neighbor Cache functions similarly to the IPv4 ARP table. Entries can be made to the Neighbor Cache by the Neighbor Discovery protocol.

The Neighbor Discovery commands allow you to set protocol parameters on an interface basis.

clear ipv6 neighbors

This command clears all the dynamically learned entries in the Neighbor Cache, or an entry on a specific interface.

Syntax

clear ipv6 neighbor [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	(Optional) Clear only the entries on the specified interface.

Defaults

None.

Mode

Router privileged exec: C3(su)->router#

Usage

To clear all dynamically learned Neighbor Cache entries, use this command without any parameters.

Example

This example clears all dynamically learned cache entries.

```
C3(su)->router#clear ipv6 neighbors
```

ipv6 nd dad attempts

This command configures the number of duplicate address detection (DAD) attempts made on the interface when configuring IPv6 unicast addresses.

Syntax

```
ipv6 nd dad attempts number
no ipv6 nd dad attempts
```

Parameters

number	Specifies the number of consecutive Neighbor Solicitation message transmitted on the interface, when Duplicate Address Detection (DAD) is performed on a unicast IPv6 address assigned to the interface. The value can range from 0 to 600. A value of 0 disables Duplicate Address Detection on the interface. A value of 1, which is the default, specifies a single transmission with no follow-up transmissions.

Defaults

Duplicate address detection enabled, for 1 attempt.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

IPv6 Duplicate Address Detection is described in RFC 2462. Duplicate Address Detection uses Neighbor Solicitation and Neighbor Advertisement messages to verify the uniqueness of an address. Duplicate Address Detection must be performed on unicast addresses prior to assigning them to an interface. An address remains in a tentative state while Duplicate Address Detection is being performed. If a tentative address is found to be a duplicate, an error message is returned and the address is not assigned to the interface.

Use this command to change the number of Neighbor Solicitation messages that can be sent for Duplicate Address Detection from the default value of 1. The **no** form of the command returns the value to the default of 1. A value of 0 disables Duplicate Address Detection on the interface.

The **show ipv6 interface** command displays the current DAD attempt setting.

Example

This example changes the number of consecutive Neighbor Solicitation messages sent for DAD to 3 on this interface.

```
C3(su)->router(Config-if(Vlan 1))# ipv6 nd dad attempts 3
```

ipv6 nd ns-interval

This command configures the interval between Neighbor Solicitations sent on an interface.

Syntax

```
ipv6 nd ns-interval {msec | 0}
no ipv6 nd ns-interval
```

Parameters

msec	Sets the interval in milliseconds between retransmissions of Neighbor Solicitation messages on the interface. The value can range from 1000 (one second) to 3,600,000 (one hour) milliseconds.
0	An advertised value of 0 means the interval is unspecified.

Defaults

By default, a value of 0 is advertised in RA messages.

Mode

Router interface configuration:C3(su)->router(Config-if(Vlan 1))#

Usage

The NS interval is used to determine the time between retransmissions of neighbor solicitation messages to a neighbor when resolving a unicast address (DAD) or when probing the reachability of a neighbor. This value is also advertised in Router Advertisement (RA) messages sent on the interface.

Use the **no** form of this command to set the interval to the default of 0.

Example

This example sets the NS interval to 2 seconds.

```
C3(su)->router(Config-if(Vlan 1))# ipv6 nd ns-interval 2000
```

ipv6 nd reachable-time

This command configures the length of time within which some reachability confirmation must be received from a neighbor for the neighbor to be considered reachable.

Syntax

```
ipv6 nd reachable-time msec
no ipv6 nd reachable-time
```

Parameters

msec	The amount of time in milliseconds that a remote IPv6 node is considered reachable. The value can range from 0 to 4,294,967,295 milliseconds. The default value is 0, which means that the time is unspecified.

Defaults

By default, a value of 0 is advertised in RA messages.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

This timer allows the C3 to detect unavailable neighbors. The shorter the time, the more quickly unavailable neighbors are detected. Very short configured times are not recommended in normal

IPv6 operation, however, because shorter times consume more IPv6 network bandwidth and processing resources.

This value is also included in all Router Advertisements messages sent out on the interface. By default, a value of 0, indicating that the configured time is unspecified by this router, is sent out in RA messages.

Use the **no** form of this command to reset this value to the default.

The **show ipv6 interface** command displays the current reachable time setting.

Example

This example sets the reachable time to 60 seconds.

```
C3(su)->router(Config-if(Vlan 1))# ipv6 nd reachable-time 60000
```

ipv6 nd other-config-flag

This command sets the "other stateful configuration" flag in router advertisements sent on this interface to true.

Syntax

```
ipv6 nd other-config-flag
no ipv6 nd other-config-flag
```

Parameters

None.

Defaults

Flag is set to false by default.

Mode

Router interface configuration: C3(su)->router(Config-if (Vlan 1))#

Usage

When the value of the "other stateful configuration" flag is true, end nodes should use stateful autoconfiguration (DHCPv6) to obtain additional information (excluding addresses). When the value is false, end nodes do not. Refer to RFC 2462, "IPv6 Stateless Address Autoconfiguration," for more information.

Use the **no** form of this command to reset the flag to false.

Example

This example sets the other stateful configuration flag to true.

```
C3(su)->router(Config-if(Vlan 1))# ipv6 nd other-config-flag
```

ipv6 nd ra-interval

This command sets the transmission interval between router advertisements.

Syntax

ipv6 nd ra-interval *sec*

no ipv6 nd ra-interval

Parameters

sec	Specifies the value in seconds of the router advertisement transmission interval. The value can range from 4 to 1800 seconds.

Defaults

600 seconds.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

The **no** form of this command resets the interval value to the default of 600 seconds.

Example

This example sets the router advertisement transmission interval to 120 seconds.

```
C3(su)->router(Config-if(Vlan 1))# ipv6 nd ra-interval 120
```

ipv6 nd ra-lifetime

This command sets the value, in seconds, that is placed in the Router Lifetime field of router advertisements sent from this interface.

Syntax

ipv6 nd ra-lifetime *sec* | **0**

no ipv6 nd ra-lifetime

Parameters

sec	Specifies the value of the Router Lifetime in seconds. The value must be 0, or an integer between the value of the router advertisement interval and 9000 seconds. A value of 0 means that this router is not to be used as the default router.

Defaults

1800 seconds.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

The **no** form of this command resets the lifetime value to the default of 1800 seconds.

Example

This example sets the router advertisement lifetime value to 3600 seconds.

```
C3(su)->router(Config-if(Vlan 1))# ipv6 nd ra-lifetime 3600
```

ipv6 nd suppress-ra

This command suppresses router advertisement transmission on this interface.

Syntax

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Parameters

None.

Defaults

Suppression disabled.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

By default, transmission of router advertisements is enabled. This command disables such transmissions. Use the **no** form of this command to re-enable transmission.

Example

This example disables router advertisement transmission.

```
C3(su)->router(Config-if(Vlan 1))# ipv6 nd suppress-ra
```

ipv6 nd prefix

This command configures the IPv6 prefixes to be included in router advertisements sent by this interface.

Syntax

ipv6 nd prefix {*ipv6-prefix/prefix-length*} [{*valid-lifetime* | **infinite**} {*preferred-lifetime* | **infinite**}] [**no-autoconfig**] [**off-link**]

no ipv6 nd prefix {*ipv6-prefix/prefix-length*}

Parameters

ipv6-prefix/prefix-length	The IPv6 network prefix and the prefix length being configured. The prefix must be in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons. The prefix length is a decimal number indicating the number of high-order contiguous bits of the address that comprise the network portion of the address.
valid-lifetime | **infinite**	(Optional) Specifies the length of time in seconds (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. The lifetime value can range from 0 to 4,294,967,295. Specifying **infinite** means that the prefix is always valid.
preferred-lifetime | **infinite**	(Optional) Specifies the length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix by means of stateless address autoconfiguration remain preferred. The lifetime value can range from 0 to 4,294,967,295. Specifying **infinite** means that the prefix is always preferred.
no-autoconfig	Unsets the autonomous address-configuration flag. When not set, means that this prefix cannot be used for autonomous address configuration. By default, the autonomous address-configuration flag is set/enabled.
off-link	Unsets the on-link flag. When not set, means that this prefix cannot be used for on-link determination. By default, the on-link flag is set/enabled.

Defaults

- Valid-lifetime — 604800
- Preferred-lifetime — 2592000
- Autoconfig — enabled
- On-link — enabled

Mode

Router interface configuration:C3(su)->router(Config-if (Vlan 1))#

Usage

Refer to RFC 2461, “Neighbor Discovery for IP Version 6,” for more information about router advertisements.

Router advertisements contain a list of prefixes used for on-link determination and/or autonomous address configuration. Flags associated with the prefixes specify the intended uses of a particular prefix. Hosts use the advertised on-link prefixes to build and maintain a list that is used in deciding when a packet’s destination is on-link or beyond a router. Hosts can use the advertised autoconfiguration prefixes to perform autonomous (stateless) address configuration, if stateless configuration is allowed (see ipv6 nd other-config-flag).

The **no** form of this command removes the prefix from the list of prefixes advertised in router advertisements by this interface.

Example

This example configures a prefix that can be used for both on-link determination and autoconfiguration, using the default values for valid lifetime and preferred lifetime.

```
C3(su)->router(Config-if(Vlan 1))# ipv6 nd prefix 2001:0db8:4444:5555/64
```

Query Commands

show ipv6

This command displays the status of IPv6 forwarding mode and unicast routing mode.

Syntax

show ipv6

Parameters

None.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Usage

The output of this command displays whether IPv6 forwarding mode and unicast routing mode are enabled or disabled.

Example

This example displays information about IPv6 modes.

```
C3(su)->router# show ipv6
IPv6 Forwarding Mode             Enabled
IPv6 Unicast Routing Mode        Enabled
```

show ipv6 interface

This command displays information about one or all configured IPv6 interfaces.

Syntax

show ipv6 interface [**vlan** *vlan-id* | **tunnel** *tunnel-id* | **loopback** *loop-id*]

Parameters

vlan *vlan-id*	(Optional) Display information only about the specified interface.
tunnel *tunnel-id*	
loopback *loop-id*	

Defaults

If no interface is specified, information about all IPv6 interfaces is displayed.

Mode

Router privileged execution: C3(su)->router#

Router global configuration: C3(su)->router(Config)#

Usage

Use this command to display the usability status of IPv6 interfaces.

If an IPv6 prefix is configured on an interface, the following information also displays:

- The IPv6 prefix and length
- The configured preferred lifetime value
- The configured valid lifetime value
- The status of the on-link flag, either enabled or disabled
- The status of the autonomous address-configuration flag (autoconfig), either enabled or disabled.

Examples

This example displays information about IPv6 interface VLAN 7.

```
C3(su)->router>show ipv6 interface vlan 7

Vlan 7 Administrative Mode                        Enabled
Vlan 7 IPv6 Routing Operational Mode              Enabled
IPv6 is                                           Enabled
IPv6 Prefix is                                    FE80::211:88FF:FE55:4A7F/128
                                        3FFE:501:FFFF:101:211:88FF:FE55:4A7F/64
                                                  3FFD::211:88FF:FE55:4A7F/64
Routing Mode                                      Enabled
Interface Maximum Transmit Unit                   1500
Router Duplicate Address Detection Transmits      1
Router Advertisement NS Interval                  0
Router Lifetime Interval                          1800
Router Advertisement Reachable Time               0
Router Advertisement Interval                     600
Router Advertisement Managed Config Flag          Enabled
Router Advertisement Other Config Flag            Enabled
Router Advertisement Suppress Flag                Disabled
```

This example displays information about IPv6 interface tunnel 1.

```
C3(su)->router>show ipv6 interface tunnel 1

Tunnel 1 Administrative Mode                      Enabled
Tunnel 1 IPv6 Routing Operational Mode            Disabled
Mode for IPv6 Tunnel                              IPv6OVER4
```

```
Source Address for IPv6 Tunnel                  192.168.1.2
Destination Address for IPv6 Tunnel             192.168.8.1
Routing Mode                                    Enabled
Interface Maximum Transmit Unit                 1480
Router Duplicate Address Detection Transmits    1
Router Advertisement NS Interval                0
Router Lifetime Interval                        1800
Router Advertisement Reachable Time             0
Router Advertisement Interval                   600
Router Advertisement Managed Config Flag        Disabled
Router Advertisement Other Config Flag          Disabled
Router Advertisement Suppress Flag              Disabled
```

show ipv6 neighbors

This command displays IPv6 Neighbor Cache information.

Syntax

show ipv6 neighbors

Parameters

None.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Usage

Use this command to display the contents of the Neighbor Cache.

Example

This example displays the neighbors in the cache.

```
C3(su)->router>show ipv6 neighbors
                                                                  Neighbor Last
IPv6 Address                            MAC Address       isRtr State    Updated
            Interface
------------------------------------ ----------------- ----- -------- -------
FE80::200:FF:FE00:A0A0                  00:00:00:00:a0:a0 False Stale       1155
            Vlan 6
FE80::2D0:B7FF:FE2C:7697                00:d0:b7:2c:76:97 False Stale       1095
            Vlan 6
FE80::2D0:B7FF:FE2C:7698                00:d0:b7:2c:76:98 False Stale       1096
            Vlan 6
FE80::2D0:B7FF:FE2C:7699                00:d0:b7:2c:76:99 False Stale       1155
            Vlan 6
FE80::2D0:B7FF:FE2C:769E                00:d0:b7:2c:76:9e False Stale       1461
            Vlan 6
FE80::2D0:B7FF:FE2C:76AA                00:d0:b7:2c:76:aa False Stale       1540
            Vlan 6
FE80::2D0:B7FF:FE2C:76AB                00:d0:b7:2c:76:ab False Stale       1553
            Vlan 6
FE80::2D0:B7FF:FE2C:76AC                00:d0:b7:2c:76:ac False Stale       1566
```

```
            Vlan 6
FE80::2D0:B7FF:FE2C:76B4                00:d0:b7:2c:76:b4 False Delay       1903
            Vlan 6
```

Table 22-1 provides an explanation of the command output.

Table 22-1 show ipv6 neighbor Output Details

Output Field	What It Displays...
IPv6 Address	The IPv6 address of the neighbor on the interface.
Interface	The interface on which this neighbor was discovered.
MAC Address	The link layer address of the neighbor.
isRtr	Whether the neighbor is a router. If the value is True, the neighbor is known to be a router. Otherwise, the value is False.
Neighbor State	State of the cache entry. Possible values are Incomplete, Reachable, Stale, Delay, Probe, and Unknown.
Last Updated	The system uptime when the information for the neighbor was last updated.

show ipv6 route

This command displays the IPv6 routing table.

Syntax

show ipv6 route [{*ipv6-addr* [*route-type*] | {{*ipv6-prefix/prefix-length* | **interface** *interface*} [*route-type*] | *route-type* | **all**]

Parameters

ipv6-addr	Specifies a specific IPv6 address for which the best-matching route should be displayed.
ipv6-prefix/prefix-length	The IPv6 network prefix of the route to display, and the prefix length. The prefix must be in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons. The prefix length is a decimal number indicating the number of high-order contiguous bits of the address that comprise the network portion of the address.
interface *interface*	Specifies that the routes with next-hops on this interface should be displayed. Interface can be of the form: **vlan** *vlan-id* **tunnel** *tunnel-id* **loopback** *loop-id*
route-type	Specifies the route type as one of the following: **connected** **static** **ospf**
all	Specifies that all routes should be displayed.

Defaults

If no parameters are entered, information about all active IPv6 routes is displayed.

Mode

Router privileged execution: C3(su)->router#

Router user execution: C3(su)->router>

Usage

Use this command to display IPv6 routing table information for active routes.

Example

This example displays all active IPv6 routes.

```
C3(su)->router>show ipv6 route

IPv6 Routing Table - 5 entries

Codes: C - connected, S - static
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2

S    ::/0 [1/0]
      via FE80::2D0:B7FF:FE2C:7694,   Vlan 6
C    3FFE:501:FFFF:100::/64 [0/0]
      via ::,   Vlan 6
C    3FFE:501:FFFF:101::/64 [0/0]
      via ::,   Vlan 7
C    3FFE:501:FFFF:108::/64 [0/0]
      via ::,   Vlan 6
S    3FFE:501:FFFF:109::/64 [1/0]
      via 3FFE:501:FFFF:100:200:FF:FE00:A1A1,   Vlan 6
      via FE80::200:FF:FE00:A1A1,   Vlan 6
```

Table 22-2 provides an explanation of the command output.

Table 22-2 show ipv6 route Output Details

Output Field	What It Displays...
Codes:	Key for the routing protocol codes that might appear in the Codes column of the routing table output.
Codes column	The code for the routing protocol that created this routing entry.
IPv6 prefix/prefix-length	The IPv6 prefix and prefix length of the destination IPv6 network corresponding to this route.
[Preference / Metric]	The administrative distance (preference) and cost (metric) associated with this route.
Tag	The decimal value of the tag associated with a redistributed route, if it is not 0.
via Next-hop	The outgoing router IPv6 address to use when forwarding traffic to the next router, if any, in the path toward the destination.
Interface	The outgoing router interface to use when forwarding traffic to the next destination.

show ipv6 route preferences

This command shows the preference value associated with the type of route.

Syntax

```
show ipv6 route preference
```

Parameters

None.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Router user execution: C3(su)->router>

Usage

Lower numbers have a greater preference. A route with a preference of 255 cannot be used to forward traffic.

The default preference value for static routes can be set with the **ipv6 route distance** command. The distance for a specific static route can be set with the **ipv6 route** command.

Note: The configuration of NSSA preferences is not supported in this release.

Example

The following example shows the output of this command.

```
C3(su)->router#show ipv6 route preferences
Local                                          0
Static                                         1
OSPF Intra                                     8
OSPF Inter                                     10
OSPF Ext T1                                    13
OSPF Ext T2                                    150
OSPF NSSA T1                                   14
OSPF NSSA T2                                   151
```

Table 22-3 provides an explanation of the command output.

Table 22-3 show ipv6 route preferences Output Details

Output Field	What It Displays...
Local	Preference of directly-connected routes.
Static	Preference of static routes.
OSPF Intra	Preference of routes within the OSPF area.
OSPF Inter	Preference of routes to other OSPF routes that are outside of the area.
OSPF Ext T1	Preference of OSPF Type-1 external routes.

Table 22-3 show ipv6 route preferences Output Details

Output Field	What It Displays...
OSPF Est T2	Preference of OSPF Type-2 external routes.
OSPF NSSA T1	Preference of OSPF NSSA Type 1 routes.
OSPF NSS! T2	Preference of OSPF NSSA Type 2 routes.

show ipv6 route summary

This command displays the summary of the routing table.

Syntax

show ipv6 route summary [**all**]

Parameters

all	(Optional) Display the count summary for all routes, including best and non-best routes.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Router user execution: C3(su)->router>

Usage

Use the command without parameters to display the count summary for only the best routes. Use **all** to display the count summary for all routes, including best and non-best routes.

Example

This example illustrates the summary information displayed by this command.

```
C3(su)->router>show ipv6 route summary all

IPv6 Routing Table Summary - 6 entries

Connected Routes                                3
Static Routes                                   3
OSPF Routes                                     0
  Intra Area Routes                             0
  Inter Area Routes                             0
  External Type-1 Routes                        0
  External Type-2 Routes                        0
Total routes                                    6

  Number of Prefixes:
    /0: 1,  /64: 5
```

Table 22-4 provides an explanation of the command output.

Table 22-4 show ipv6 summary Output Details

Output Field	What It Displays...
Connected Routes	Total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
OSPF Routes	Total number of routes installed by OSPFv3 protocol.
Number of Prefixes	Summarizes the number of routes with prefixes of different lengths
Total Routes	Total number of routes in the routing table.

show ipv6 traffic

Use this command to show traffic and statistics for IPv6 and ICMPv6.

Syntax

show ipv6 traffic [*interface*]

Parameters

interface	(Optional) Specifies the interface for which traffic information should be displayed. Interface can be of the form: **vlan** *vlan-id* **tunnel** *tunnel-id* **loopback** *loop-id*

Defaults

If no interface is specified, information about traffic on all interfaces is displayed.

Mode

Router privileged execution: C3(su)->router#

Usage

Specify a logical, loopback, or tunnel interface to view information about traffic on a specific interface. If you do not specify an interface, the command displays information about traffic on all interfaces.

Example

The following example displays the output of this command.

```
C3(su)->router>show ipv6 traffic
IPv6 STATISTICS
Total Datagrams Received..................................... 116
Received Datagrams Locally Delivered......................... 116
Received Datagrams Discarded Due To Header Errors......... 0
Received Datagrams Discarded Due To MTU.................... 0
Received Datagrams Discarded Due To No Route.............. 0
Received Datagrams With Unknown Protocol................... 0
Received Datagrams Discarded Due To Invalid Address....... 0
Received Datagrams Discarded Due To Truncated Data........ 0
Received Datagrams Discarded Other......................... 0
```

```
Received Datagrams Reassembly Required..................... 0
Datagrams Successfully Reassembled......................... 0
Datagrams Failed To Reassemble............................. 0
Datagrams Forwarded........................................ 0
Datagrams Locally Transmitted.............................. 876
Datagrams Transmit Failed.................................. 0
Datagrams Successfully Fragmented.......................... 0
Datagrams Failed To Fragment............................... 0
Fragments Created.......................................... 0
Multicast Datagrams Received............................... 17
Multicast Datagrams Transmitted............................ 547

ICMPv6 STATISTICS
Total ICMPv6 Messages Received............................. 116
ICMPv6 Messages With Errors Received....................... 4
ICMPv6 Destination Unreachable Messages Received.......... 0
ICMPv6 Messages Prohibited Administratively Received...... 0
ICMPv6 Time Exceeded Messages Received..................... 0
ICMPv6 Parameter Problem Messages Received................. 0
ICMPv6 Packet Too Big Messages Received.................... 0
ICMPv6 Echo Request Messages Received...................... 52
ICMPv6 Echo Reply Messages Received........................ 0
ICMPv6 Router Solicit Messages Received.................... 0
ICMPv6 Router Advertisement Messages Received.............. 5
ICMPv6 Neighbor Solicit Messages Received.................. 31
ICMPv6 Neighbor Advertisement Messages Received............ 28
ICMPv6 Redirect Messages Received.......................... 0
ICMPv6 Group Membership Query Messages Received............ 0
ICMPv6 Group Membership Response Messages Received......... 0
ICMPv6 Group Membership Reduction Messages Received........ 0
Total ICMPv6 Messages Transmitted.......................... 876
ICMPv6 Messages Not Transmitted Due To Error............... 0
ICMPv6 Destination Unreachable Messages Transmitted........ 0
ICMPv6 Messages Prohibited Administratively Transmitted... 0
ICMPv6 Time Exceeded Messages Transmitted.................. 0
ICMPv6 Parameter Problem Messages Transmitted.............. 0
ICMPv6 Packet Too Big Messages Transmitted................. 0
ICMPv6 Echo Request Messages Transmitted................... 157
ICMPv6 Echo Reply Messages Transmitted..................... 52
ICMPv6 Router Solicit Messages Transmitted................. 0
ICMPv6 Router Advertisement Messages Transmitted........... 7
ICMPv6 Neighbor Solicit Messages Transmitted............... 625
ICMPv6 Neighbor Advertisement Messages Transmitted......... 27
ICMPv6 Redirect Messages Transmitted....................... 0
ICMPv6 Group Membership Query Messages Transmitted......... 0
ICMPv6 Group Membership Response Messages Transmitted..... 8
ICMPv6 Group Membership Reduction Messages Transmitted.... 0
ICMPv6 Duplicate Address Detects........................... 0
```

Table 22-5 provides an explanation of the command output.

Table 22-5 show ipv6 traffic Output Details

Output Field	What It Displays...
Total Datagrams Received	Total number of input datagrams received by the interface, including those received in error.
Received Datagrams Locally Delivered	Total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter increments at the interface to which these datagrams were addressed, which might not necessarily be the input interface for some of the datagrams.

Table 22-5 show ipv6 traffic Output Details (Continued)

Output Field	What It Displays...
Received Datagrams Discarded Due To Header Errors	Number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.
Received Datagrams Discarded Due To MTU	Number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
Received Datagrams Discarded Due To No Route	Number of input datagrams discarded because no route could be found to transmit them to their destination.
Received Datagrams With Unknown Protocol	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the datagrams.
Received Datagrams Discarded Due To Invalid Address	Number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, ::0) and unsupported addresses (for example, addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Received Datagrams Discarded Due To Truncated Data	Number of input datagrams discarded because datagram frame didn't carry enough data.
Received Datagrams Discarded Other	Number of input IPv6 datagrams for which no problems were encountered to prevent their continue processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include datagrams discarded while awaiting re-assembly.
Received Datagrams Reassembly Required	Number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Successfully Reassembled	Number of IPv6 datagrams successfully reassembled. Note that this counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Failed To Reassemble	Number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in by combining them as they are received. This counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Forwarded	Number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface increments.

Table 22-5 show ipv6 traffic Output Details (Continued)

Output Field	What It Displays...
Datagrams Locally Transmitted	Total number of IPv6 datagrams which local IPv6 user protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams.
Datagrams Transmit Failed	Number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipv6IfStatsOutForwDatagrams if any such packets met this (discretionary) discard criterion.
Datagrams Successfully Fragmented	Number of IPv6 datagrams that have been successfully fragmented at this output interface.
Datagrams Failed To Fragment	Number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
Fragments Created	Number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
Multicast Datagrams Received	Number of multicast packets received by the interface.
Multicast Datagrams Transmitted	Number of multicast packets transmitted by the interface.
Total ICMPv6 Messages Received	Total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
ICMPv6 Messages with Errors Received	Number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
ICMPv6 Destination Unreachable Messages Received	Number of ICMP Destination Unreachable messages received by the interface.
ICMPv6 Messages Prohibited Administratively Received	Number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPv6 Time Exceeded Messages Received	Number of ICMP Time Exceeded messages received by the interface.
ICMPv6 Parameter Problem Messages Received	Number of ICMP Parameter Problem messages received by the interface.
ICMPv6 Packets Too Big Messages Received	Number of ICMP Packet Too Big messages received by the interface.
ICMPv6 Echo Request Messages Received	Number of ICMP Echo (request) messages received by the interface.
ICMPv6 Echo Reply Messages Received	Number of ICMP Echo Reply messages received by the interface.
ICMPv6 Router Solicit Messages Received	Number of ICMP Router Solicit messages received by the interface.
ICMPv6 Router Advertisement Messages Received	Number of ICMP Router Advertisement messages received by the interface.

Table 22-5 show ipv6 traffic Output Details (Continued)

Output Field	What It Displays...
ICMPv6 Neighbor Solicit Messages Received	Number of ICMP Neighbor Solicit messages received by the interface.
ICMPv6 Neighbor Advertisement Messages Received	Number of ICMP Neighbor Advertisement messages received by the interface.
ICMPv6 Redirect Messages Received	Number of Redirect messages received by the interface.
ICMPv6 Group Membership Query Messages Received	Number of ICMPv6 Group Membership Query messages received.
ICMPv6 Group Membership Response Messages Received	Number of ICMPv6 group Membership Response messages received.
ICMPv6 Group Membership Reduction Messages Received	Number of ICMPv6 Group Membership Reduction messages received.
Total ICMPv6 Messages Transmitted	Total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
ICMPv6 Messages Not Transmitted Due To Error	Number of ICMP messages which this interface did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
ICMPv6 Destination Unreachable Messages Transmitted	Number of ICMP Destination Unreachable messages sent by the interface.
ICMPv6 Messages Prohibited Administratively Transmitted	Number of ICMP destination unreachable/communication administratively prohibited messages sent.
ICMPv6 Time Exceeded Messages Transmitted	Number of ICMP Time Exceeded messages sent by the interface.
ICMPv6 Parameter Problem Messages Transmitted	Number of ICMP Parameter Problem messages sent by the interface.
ICMPv6 Packet Too Big Messages Transmitted	Number of ICMP Packet Too Big messages sent by the interface.
ICMPv6 Echo Request Messages Transmitted	Number of ICMP Echo (request) messages sent by the interface.ICMP echo messages sent
ICMPv6 Echo Reply Messages Transmitted	Number of ICMP Echo Reply messages sent by the interface.
ICMPv6 Router Solicit Messages Transmitted	Number of ICMP Router Solicitation messages sent by the interface.
ICMPv6 Router Advertisement Messages Transmitted	Number of ICMP Router Advertisement messages sent by the interface.
ICMPv6 Neighbor Solicit Messages Transmitted	Number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Neighbor Advertisement Messages Transmitted	Number of ICMP Neighbor Advertisement messages sent by the interface.
ICMPv6 Redirect Messages Transmitted	Number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.

Table 22-5 show ipv6 traffic Output Details (Continued)

Output Field	What It Displays...
ICMPv6 Group Membership Query Messages Transmitted	Number of ICMPv6 Group Membership Query messages sent.
ICMPv6 Group Membership Response Messages Transmitted	Number of ICMPv6 group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Transmitted	Number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	Number of duplicate addresses detected by the interface

clear ipv6 statistics

This command clears IPv6 statistics for all interfaces or a specific interface.

Syntax

clear ipv6 statistics [*interface*]

Parameters

interface	(Optional) Specifies the interface for statistics should be cleared. Interface can be of the form: **vlan** *vlan-id* **tunnel** *tunnel-id* **loopback** *loop-id*

Defaults

If no interface is specified, statistics are cleared (reset to 0) for all interfaces.

Mode

Router privileged executionC3(su)->router#

Usage

IPv6 statistics are displayed with the **show ipv6 traffic** command. If no interface is specified, the counters for all IPv6 traffic statistics are reset to zero when this command is executed.

Example

This example clears the statistics for VLAN 6.

```
C3(su)->router# clear ipv6 statistics vlan 6
```

23

IPv6 Proxy Routing

This chapter describes the commands used to enable IPv6 proxy routing and the suggested procedure to configure a mixed C2 and C3 stack to use IPv6 proxy routing.

Overview

IPv6 proxy routing allows a mixed C2/C3 stack to support some IPv6 routing functionality. When IPv6 proxy routing is enabled, all the switches in the stack can support IPv6 unicast routing and IPv6 tunneling. You can configure port-based and VLAN-based IPv6 routing interfaces on any C2 or C3 stack unit. There is no change in existing IPv4 routing capabilities.

Since this is a function that exists only in a mixed stack, it is implemented only in the C2 firmware, release 5.01 and later. For IPv6 proxy routing to exist in the stack, a C3 unit must run as the manager of the stack. To facilitate this, the stack manager preference of C3 units should be set to a higher value than C2 units. If a C3 unit is added to an all C2 stack, you must move the manager to a C3 unit to use this feature.

Multiple C3 units can exist in the mixed stack. All the C3 units in the mixed stack will independently perform hardware IPv6 routing/tunneling. The manager C3 unit will transparently do the hardware IPv6 routing/tunneling for all the C2 units.

When IPv6 proxy routing is enabled, the C2 being configured for routing/tunneling (called the proxy client) is configured to redirect the routed IPV6/Tunneling packets to one of the stacking ports of the C3 stack manager (called the proxy server). The C2 is only configured if the proxy feature is already enabled on the stack. It should be noted that only IPv6 packets with a destination MAC of the router MAC of the system are redirected to the proxy server.

On the proxy server, all incoming packets to the stacking ports with a destination of one of the stacking ports will be processed through L2 and L3 switching logic. If the destination port is not one of the stacking ports (not an IPv6 packet), then the incoming packet is forwarded based on header information.

This feature is disabled by default.

In order to use the OSPF, PIM-SM, DVMRP, or VRRP protocols, you must have purchased and installed the C2 advanced routing license.

Limitations

- Proxy routing will use up to two masks in the fast forwarding processor associated with each port involved in routing of IPv6 packets. This will require restrictions on the use of policy when proxy routing is enabled.
- All IPv6 packets ingressing or egressing a C2 port must be sent over the stack to the C3 stack master. Limited stack bandwidth and the amount of IPv6 traffic must be carefully considered when configuring multiple C2 ports for IPv6 routing.
- If the stack master moves from a C3 unit to a C2 unit in the stack, proxy routing will no longer be available. To ensure that proxy routing continues to operate in the event of a failover, C3 units must be configured to be preferred when a new master is elected.

Preparing a Mixed Stack for IPv6 Proxy Routing

At least two C3 switches should be added to a C2 stack, for management redundancy.

As in any mixed C2/C3 mixed stack, the C2 firmware (release 5.01 or later) must be installed on the C3 switches. Refer to "Issues Related to Mixed Type Stacks" on page 2-5 for additional information.

If you are adding the C3 switches to an existing C2 stack, make one of the C3 switches the stack manager. For example, if the current stack manager is unit 1 and the C3 switch that you want to become manager is unit 7:

```
C2(su)->set switch movemenagement 1 7
Moving stack management will unconfigure entire stack including all interfaces.
Are you sure you want to move stack management? (y/n) y
```

Set the management priority of the C3 switches to be higher than that of the C2 switches. For example, if your C3 switches are units 7 and 8, and you want the unit 7 C3 switch to always become the manager and the unit 8 C3 switch to be the backup manager:

```
C2(su)->set switch 7 priority 15
C2(su)->set switch 8 priority 13
```

Use the **show switch** *unit* command to display switch priority (Admin Management Preference).

```
C2(su)->show switch 7
Switch                          7
Management Status               Management Switch
Hardware Management Preference  Unassigned
Admin Management Preference     15
Switch Type                     C3G124-48
Preconfigured Model Identifier  C3G124-48
Plugged-in Model Identifier     C3G124-48
Switch Status                   OK
Switch Family                   XGS3
Switch Description
Detected Code Version           05.02.00.0031
Detected Code in Flash          05.02.00.0031
Detected Code in Back Image     05.01.06.0006
Up Time                         0 days 0 hrs 13 mins 9 secs
```

Commands

ipv6 proxy-routing

Use this command to enable or disable IPv6 proxy routing on a mixed C2/C3 stack.

Syntax

ipv6 proxy-routing

no ipv6 proxy-routing

Parameters

None.

Defaults

IPv6 proxy routing is disabled by default.

Mode

Router global configuration: C2(su)->router(Config)#

Usage

IPv6 proxy routing is disabled by default. It must be enabled with this command before the C2 switches in the stack will start redirecting routed IPv6/tunneling packets to the C3 proxy server.

Uses the **no** form of this command to disable IPv6 proxy routing.

Example

This example enables IPv6 proxy routing.

```
c2(su)->router
c2(su)->router>enable
c2(su)->router#config
Enter configuration commands:
c2(su)->router(Config)#ipv6 proxy-routing
```

show ipv6 proxy-routing

Use this command to display the status of IPv6 proxy routing.

Syntax

show ipv6 proxy-routing

Parameters

None.

Defaults

None.

Mode

Any routing mode.

Example

This example shows the output of this command when IPv6 proxy routing is disabled.

```
c2(su)->router(Config)#show ipv6 proxy-routing
IPv6 Proxy Routing Mode.............................. Disable
```

24

DHCPv6 Configuration

*** IPv6 Routing License Required ***

IPv6 routing must be enabled with a license key in order to use this feature. If you have purchased an IPv6 routing license key, and have enabled routing on the device, you must activate your license as described in the chapter entitled “Activating Licensed Features” in order to enable the DHCPv6 configuration command set. If you wish to purchase an IPv6 routing license, contact Enterasys Networks Sales.

The commands described in this chapter perform configuration of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) on the SecureStack C3.

Overview

DHCP is generally used between clients (for example, hosts) and servers (for example, routers) for the purpose of assigning IP addresses, gateways, and other networking definitions such as DNS, NTP, and/or SIP parameters. However, IPv6 natively provides for auto-configuration of IP addresses through the IPv6 Neighbor Discovery Protocol (NDP) and the use of Router Advertisement messages. Thus, the role of DHCPv6 within the network is different from DHCPv4 in that it is less relied upon for IP address assignment.

DHCPv6 server and client interactions are described by RFC 3315. There are many similarities between DHCPv6 and DHCPv4 interactions and options, but the messages and option definitions are sufficiently different. There is no migration or inter-operability from DHCPv4 to DHCPv6.

DHCPv6 incorporates the notion of the stateless server, where DHCPv6 is not used for IP address assignment to a client. Instead, it only provides other networking information such as DNS, NTP, and/or SIP information. The stateless server behavior is described by RFC 3736, which simply contains descriptions of the portions of RFC 3315 that are necessary for stateless server behavior.

In order for a router to drive a DHCPv6 client to utilize stateless DHCPv6, the “other stateful configuration” option must be configured for neighbor discovery on the corresponding IPv6 router interface. This in turn causes DHCPv6 clients to send the DHCPv6 “Information Request” message in response. A DHCPv6 server then responds by providing only networking definitions such as DNS domain name and server definitions, NTP server definitions, and/or SIP definitions.

RFC 3315 also describes DHCPv6 Relay Agent interactions, which are very much like DHCPv4 Relay Agent. RFC 3046 describes the DHCPv6 Relay Agent Information Option, which employs very similar capabilities as those described by DHCPv4 Relay Agent Option in RFC 2132.

With the larger address space inherent to IPv6, addresses within a network can be allocated more effectively in a hierarchical fashion. DHCPv6 introduces the notion of "prefix delegation" as described in RFC 3633 as a way for routers to centralize and delegate IP address assignment.

Default Conditions

The following table lists the default DHCPv6 conditions.

Condition	Default Value
IPv6 DHCP	Disabled
IPv6 DHCP Relay Agent Information Option	32
IPv6 DHCP Relay Agent Information Remote ID Sub-option	1
IPv6 DHCP Preferred Lifetime	2592000 seconds
IPv6 DHCP Valid Lifetime	604800 seconds

Global Configuration Commands

Purpose

These router global configuration mode commands are used to enable DHCPv6 on the router, configure relay agent global parameters, and enter DHCP pool configuration mode.

Commands

For information about...	Refer to page...
ipv6 dhcp enable	24-2
ipv6 dhcp relay-agent-info-opt	24-3
ipv6 dhcp relay-agent-info-remote-id-subopt	24-4
ipv6 dhcp pool	24-4

ipv6 dhcp enable

This command enables DHCPv6 on the router.

Syntax

`ipv6 dhcp enable`

`no ipv6 dhcp enable`

Parameters

None.

Defaults

By default, DHCPv6 is disabled.

Mode

Router global configuration: C3(su)->router(Config)#

Usage

Use this command to enable DHCPv6 on the router. Use the **no** form of this command to disable DHCPv6 after it has been enabled.

Example

This example enables DHCPv6.

```
C3(su)->router(Config)# ipv6 dhcp enable
```

ipv6 dhcp relay-agent-info-opt

This command configures a number to represent the DHCPv6 Relay Agent Information Option.

Syntax

ipv6 dhcp relay-agent-info-opt *option*

Parameters

option	The value of *option* may range from 32 to 65535. The default value is 32.

Defaults

The default value of the DHCPv6 Relay Agent Information Option is 32.

Mode

Router global configuration: C3(su)->router(Config)#

Usage

The DHCPv6 Relay Agent Information Option allows for various sub-options to be attached to messages that are being relayed by the local router to a relay server. The relay server may in turn use this information in determining an address to assign to a DHCPv6 client. Refer to RFC 3046 for more information.

Example

This example sets the Relay Agent Information Option value to 82.

```
C3(su)->router(Config)# ipv6 dhcp relay-agent-info-opt 82
```

ipv6 dhcp relay-agent-info-remote-id-subopt

This command configures a number to represent the DHCPv6 Relay Agent Remote-ID sub-option.

Syntax

ipv6 dhcp relay-agent-info-remote-id-subopt *option*

Parameters

option	The value of *option* may range from 1 to 65535. The default value is 1.

Defaults

The default value of the DHCPv6 Relay Agent Remote-ID sub-option is 1.

Mode

Router global configuration: C3(su)->router(Config)#

Usage

This sub-option may be added by DHCP relay agents which terminate switched or permanent circuits and have mechanisms to identify the remote host end of the circuit. Refer to RFC 3046 for more information.

Example

This example sets the Relay Agent Remote-ID sub-option value to 2.

```
C3(su)->router(Config)# ipv6 dhcp relay-agent-info-remote-id-subopt 2
```

ipv6 dhcp pool

This command allows you to enter IPv6 DHCP pool configuration mode for the specified pool name.

Syntax

ipv6 dhcp pool *pool-name*

no ipv6 dhcp pool *pool-name*

Parameters

pool-name	Specifies the name of the pool to be configured. Pool names must be less than 31 alpha-numeric characters.

Defaults

None.

Mode

Router global configuration: C3(su)->router(Config)#

Usage

DHCPv6 pools are used to specify information for the DHCPv6 server to distribute to DHCPv6 clients. These pools are shared between multiple interfaces over which DHCPv6 server capabilities are configured.

After executing this command and entering pool configuration mode, you can return to global configuration mode by executing the **exit** command. Pool configuration commands are described in the section "Address Pool Configuration Commands" on page 24-6.

Use the **no** form of this command to remove a specified pool.

Example

This example enters DHCP pool configuration mode to configure the pool named "PoolA."

```
C3(su)->router(Config)# ipv6 dhcp pool PoolA
C3(su)->router(Config-dhcp6s-pool)#
```

Address Pool Configuration Commands

Purpose

These DHCP pool configuration mode commands are used to configure address pool parameters. This information is provided to DHCP clients by the DHCP server.

Commands

domain-name

This command sets the DNS domain name which is provided to DHCPv6 clients by the DHCPv6 server.

Syntax

domain-name *name*

no domain-name *name*

Parameters

name	Specifies the DNS domain name for the pool being configured. The name can consist of no more than 31 alpha-numeric characters.

Defaults

None.

Mode

Router DHCPv6 pool configuration mode: C3(su)->router(Config-dhcp6s-pool)#

Usage

A DNS domain name is configured for stateless server support. A DHCPv6 pool can have up to 8 domain names configured for it.

The **no** form of this command will remove the domain name from the DHCPv6 pool being configured.

Example

This example specifies the domain name “enterasys.com” for the pool named PoolA.

```
C3(su)->router(Config)# ipv6 dhcp pool PoolA
C3(su)->router(Config-dhcp6s-pool)# domain-name enterasys.com
```

dns-server

This command sets the IPv6 DNS server address which is provided to DHCPv6 clients by the DHCPv6 server.

Syntax

dns-server *server-address*

no dns-server *server-address*

Parameters

server-address	The IPv6 address of the DNS server. This parameter must be in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons.

Defaults

None.

Mode

Router DHCPv6 pool configuration mode: C3(su)->router(Config-dhcp6s-pool)#

Usage

A DNS server address is configured for stateless server support. A DHCPv6 pool can have up to 8 DNS server addresses configured for it.

The **no** form of this command will remove the DHCPv6 server address from the DHCPv6 pool being configured.

Example

This example configures a DNS server address for the pool named PoolA.

```
C3(su)->router(Config)# ipv6 dhcp pool PoolA
C3(su)->router(Config-dhcp6s-pool)# dns-server 2001:0db8:1234:5678::A
```

prefix-delegation

This command configures a numeric prefix to be delegated to a specified prefix delegation client.

Syntax

prefix-delegation *prefix/prefix-length DUID* [**name** *hostname*] [**valid-lifetime** {*secs* | **infinite**}] [**preferred-lifetime** {*secs* | **infinite**}]

no prefix-delegation *prefix/prefix-length DUID*

Parameters

prefix/prefix-length	This *prefix* must be in the form documented in RFC 4291, with the address specified in hexadecimal using 16-bit values between colons. The value of *prefix-length* is a decimal number indicating the number of high-order contiguous bits of the address that comprise the prefix.
DUID	The DHCP Unique Identifier (DUID) of the prefix delegation client, as described in RFC 3315.
name *hostname*	(Optional) The name of the prefix delegation client, consisting of up to 31 alpha-numeric characters. This name is used for logging and/or tracing only.
valid-lifetime *secs* | **infinite**	(Optional) The valid lifetime of the prefix, specified as seconds or as **infinite**. The value of *secs* can range from 0 to 4294967295.
preferred-lifetime *secs* | **infinite**	(Optional) The preferred lifetime of the prefix, specified as seconds or as **infinite**. The value of *secs* can range from 0 to 4294967295.

Defaults

Default value of valid lifetime of prefix: 604,800

Default value of preferred lifetime of prefix: 2,592,000

Mode

Router DHCPv6 pool configuration mode: C3(su)->router(Config-dhcp6s-pool)#

Usage

Use this command to manually configure an IPv6 address prefix to be delegated to a specific client, identified by their DHCP unique identifier. Refer to RFC 3633, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6," for more information about prefix delegation.

Use the **no** form of this command to remove a configured prefix.

Example

This example configures a prefix to be delegated to the prefix delegation client identified by the DUID 00:02:00:00:00:11:0A:C0:89:D3:03:00:09:AA. The default lifetime values are used.

```
C3(su)->router(Config)# ipv6 dhcp pool PoolA
C3(su)->router(Config-dhcp6s-pool)# prefix-delegation 2001:0db8:10::/48
00:02:00:00:00:11:0A:C0:89:D3:03:00:09:AA
```

exit

This command exits from DHCPv5 pool configuration mode and returns to global configuration mode.

Syntax

```
exit
```

Parameters

None.

Defaults

None.

Mode

Router DHCPv6 pool configuration mode: C3(su)->router(Config-dhcp6s-pool)#

Example

This example illustrates how to exit DHCPv6 pool configuration mode.

```
C3(su)->router(Config-dhcp6s-pool)# exit
C3(su)->router(Config)#
```

Interface Configuration Commands

Purpose

These commands are used to configure an interface as either a DHCPv6 server or a DHCPv6 relay agent.

Commands

ipv6 dhcp server

This command configures DHCPv6 server functionality on an interface.

Syntax

ipv6 dhcp server *pool-name* [**rapid-commit**} [**preference** *pref*]

no ipv6 dhcp server *pool-name*

Parameters

pool-name	Specifies the pool containing stateless and/or prefix delegation parameters that should be used by the DHCPv6 server. Refer to "Address Pool Configuration Commands" on page 24-6 for the commands to configure an address pool.
rapid-commit	(Optional) Specify that the server should use the Rapid Commit option that allows for an abbreviated exchange between DHCPv6 client and server. Refer to RFC 3315 for more information.
preference *pref*	(Optional) Specifies the value of the server's Preference option. This value, which can range from 0 to 4,294,967,295, is used by clients to determine preference among multiple DHCPv6 servers.

Defaults

By default, DHCPv6 functionality is disabled.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

Use this command to configure DHCPv6 server parameters when an interface will act as a DHCPv6 server. Address pools are configured using the commands described in section "Address Pool Configuration Commands" on page 24-6.

An interface can be configured as either a DHCPv6 server or a DHCPv6 relay agent, but not both.

Use the **no** form of this command to remove DHCPv6 server functionality from an interface.

Example

This example configures routing interface VLAN 7 to be a DHCPv6 server, using the address pool named PoolA.

```
C3(su)->router(Config)# interface vlan 7
C3(su)->router(Config-if(Vlan 7))# ipv6 dhcp server PoolA
```

ipv6 dhcp relay

This command configures an interface for DHCPv6 relay agent functionality.

Syntax

ipv6 dhcp relay {**destination** *dest-addr* **interface** *intf* | **interface** *intf*} [**remote-id** {**duid-ifid** | *user-defined-string*}]

no ipv6 dhcp relay {**destination** *dest-addr* **interface** *intf* | **interface** *intf*}

Parameters

destination *dest-addr*	Specifies the IPv6 address of a DHCPv6 relay server. This IPv6 address can be a global address, a multicast address, or a link-local address. If the address is a multicast or link-local address, then you must specify the interface to be used to contact the relay server with the **interface** parameter.
interface *intf*	Specifies the interface to be used to contact the relay server. The interface is identified by port type.unit number.port number. For example, ge.3.1. If **destination** *dest-addr* is not specified, then an interface must be specified and the DHCPV6-ALL-AGENTS multicast address (FF02::1:2) is used to relay DHCPv6 messages to the relay server.
remote-id {**duid-ifid** | *user-defined-string*}	(Optional) Specifies that the Relay Agent Information Option Remote-ID sub-option is to be added to relayed messages. Specifying **duid-ifid** causes the remote ID to be derived from the relay agent's DUID and the relay interface number. Alternatively, you can specify the remote ID as a *user-defined-string* of alpha-numeric characters. Refer to RFC 3046 and RFC 4649 for more information about the Remote-ID option.

Defaults

If **remote-id** is not specified, the Relay Agent Information Option Remote-ID sub-option is not added to relayed messages.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

Use this command to configure a routing interface as a DHCPv6 relay agent.

An interface can be configured as either a DHCPv6 server or a DHCPv6 relay agent, but not both.

Use the **no** form of this command to remove DHCPv6 relay agent functionality from an interface.

Examples

This example configures interface VLAN 8 as a DHCPv6 relay agent that relays DHCPv6 messages to the DHCPv6 server at the global address 2001:0db8:1234:5555::122:10.

```
C3(su)->router(Config)# interface vlan 8
C3(su)->router(Config-if(Vlan 8))# ipv6 dhcp relay destination
2001:0db8:1234:5555::122:10/64
```

This example configures interface VLAN 8 as a DHCPv6 relay agent by configuring the interface through which the relay agent relays messages using the DHCPV6-ALL-AGENTS multicast address.

```
C3(su)->router(Config)# interface vlan 8
C3(su)->router(Config-if(Vlan 8))# ipv6 dhcp relay interface ge.3.1
```

DHCPv6 Show Commands

Purpose

These commands are used to display DHCPv6 configuration information and statistics, to clear statistics globally or for a specific interface, and to display address pool and binding information.

Commands

show ipv6 dhcp

This command displays the state of DHCPv6 on the switch and, if DHCPv6 is enabled, the switch's DHCP unique identifier (DUID).

Syntax

```
show ipv6 dhcp
```

Parameters

None.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Example

This example illustrates the output of this command when DHCPv6 is enabled on the switch.

```
C3(su)->router# show ipv6 dhcp
DHCPv6 is enabled
Server DUID: 00:01:00:06:90:83:57:c7:00:11:88:56:5d:58
```

show ipv6 dhcp interface

This command displays DHCPv6 configuration information or DHCPv6 statistics for the specified routing interface.

Syntax

show ipv6 dhcp vlan *vlan-id* [**statistics**]

Parameters

vlan *vlan-id*	Specifies the ID of the routing interface for which to display DHCPv6 information.
statistics	(Optional) Specifies that DHCPv6 statistics for the specified interface should be displayed.

Defaults

If **statistics** is not specified, configuration information about the interface is displayed.

Mode

Router privileged execution: C3(su)->router#

Usage

When you display DHCPv6 configuration information, the information displayed is different depending on whether the interface has been configured as a DHCPv6 server or relay agent.

Examples

This example displays DHCPv6 configuration information about VLAN 80, which was configured as a DHCPv6 server.

```
C3(su)->router# show ipv6 dhcp interface vlan 80
IPv6 Interface                                  Vlan 80
Mode                                            Server
Pool Name                                       newpool
Server Preference                               5
Option Flags                                    Rapid Commit
```

This example displays DHCPv6 configuration information about VLAN 10, which was configured as a relay agent. The output fields are described in Table 24-1 on page 24-15.

```
C3(su)->router# show ipv6 dhcp interface vlan 10
IPv6 Interface                                  Vlan 10
Mode                                            Relay
Relay Address                                   5006:4567::100:1
Relay Interface Number
Relay Remote ID
Option Flags
```

Table 24-1 provides an explanation of the command output.

Table 24-1 Output of show ipv6 dhcp interface Command

Output...	What it displays...
IPv6 Interface	Shows the interface name.
Mode	Shows whether the interface is an IPv6 DHCP relay agent or server.
Pool Name	Displays when interface is a server. Shows the pool name specifying information for DHCPv6 server distribution to DHCPv6 clients.
Server Preference	Displays when interface is a server. Shows the preference of the server.
Option Flags	Displays when interface is a server. Shows whether rapid commit is enabled.
Relay Address	Displays when interface is a relay agent. Shows the IPv6 address of the relay server.
Relay Interface Number	Displays when interface is a relay agent. Shows the relay server interface in *port type.unit number.port number* format.
Relay Remote ID	Displays when interface is a relay agent. If configured, shows the contents of the remote-id field for the Remote-ID option.
Option Flags	Displays when interface is a relay agent. Shows whether rapid commit is configured.

This example displays the DHCPv6 statistics for VLAN 80.

```
C3(su)->router# show ipv6 dhcp interface vlan 80 statistics

DHCPv6 Interface Vlan 80 Statistics
-----------------------------------
DHCPv6 Solicit Packets Received                0
DHCPv6 Request Packets Received                0
DHCPv6 Confirm Packets Received                0
DHCPv6 Renew Packets Received                  0
DHCPv6 Rebind Packets Received                 0
DHCPv6 Release Packets Received                0
DHCPv6 Decline Packets Received                0
DHCPv6 Inform Packets Received                 0
DHCPv6 Relay-forward Packets Received          0
DHCPv6 Relay-reply Packets Received            0
DHCPv6 Malformed Packets Received              0
Received DHCPv6 Packets Discarded              0
Total DHCPv6 Packets Received                  0
DHCPv6 Advertisement Packets Transmitted       0
DHCPv6 Reply Packets Transmitted               0
DHCPv6 Reconfig Packets Transmitted            0
DHCPv6 Relay-reply Packets Transmitted         0
DHCPv6 Relay-forward Packets Transmitted       0
Total DHCPv6 Packets Transmitted               0
```

Table 24-2 provides an explanation of the command output.

show ipv6 dhcp statistics

This command displays IPv6 DHCP statistics for all interfaces.

Syntax

show ipv6 dhcp statistics

Parameters

None.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Example

This example displays the output of this command.

```
C3(su)->router# show ipv6 dhcp statistics

DHCPv6 Interface Global Statistics
----------------------------------
DHCPv6 Solicit Packets Received                0
DHCPv6 Request Packets Received                0
DHCPv6 Confirm Packets Received                0
DHCPv6 Renew Packets Received                  0
DHCPv6 Rebind Packets Received                 0
DHCPv6 Release Packets Received                0
DHCPv6 Decline Packets Received                0
DHCPv6 Inform Packets Received                 0
DHCPv6 Relay-forward Packets Received          0
DHCPv6 Relay-reply Packets Received            0
DHCPv6 Malformed Packets Received              0
Received DHCPv6 Packets Discarded              0
Total DHCPv6 Packets Received                  0
DHCPv6 Advertisement Packets Transmitted       0
DHCPv6 Reply Packets Transmitted               0
DHCPv6 Reconfig Packets Transmitted            0
DHCPv6 Relay-reply Packets Transmitted         0
DHCPv6 Relay-forward Packets Transmitted       0
Total DHCPv6 Packets Transmitted               0
```

Table 24-2 provides an explanation of the command output.

Table 24-2 Output of show ipv6 dhcp statistics Command

Output...	What it displays...
DHCPv6 Solicit Packets Received	Number of solicit received statistics.
DHCPv6 Request Packets Received	Number of request received statistics.
DHCPv6 Confirm Packets Received	Number of confirm received statistics.
DHCPv6 Renew Packets Received	Number of renew received statistics.
DHCPv6 Rebind Packets Received	Number of rebind received statistics.
DHCPv6 Release Packets Received	Number of release received statistics.

Table 24-2 Output of show ipv6 dhcp statistics Command (Continued)

Output...	What it displays...
DHCPv6 Decline Packets Received	Number of decline received statistics.
DHCPv6 Inform Packets Received	Number of inform received statistics.
DHCPv6 Relay-forward Packets Received	Number of relay forward received statistics.
DHCPv6 Relay-reply Packets Received	Number of relay-reply received statistics.
DHCPv6 Malformed Packets Received	Number of malformed packets statistics.
Received DHCPv6 Packets Discarded	Number of DHCP discarded statistics.
Total DHCPv6 Packets Received	Total number of DHCPv6 received statistics.
DHCPv6 Advertisement Packets Transmitted	Number of advertise sent statistics.
DHCPv6 Reply Packets Transmitted	Number of reply sent statistics.
DHCPv6 Reconfig Packets Transmitted	Number of reconfigure sent statistics.
DHCPv6 Relay-reply Packets Transmitted	Number of relay-reply sent statistics.
DHCPv6 Relay-forward Packets Transmitted	Number of relay-forward sent statistics.
Total DHCPv6 Packets Transmitted	Total number of DHCPv6 sent statistics.

clear ipv6 dhcp statistics

This command clears IPv6 DHCP statistics, either all statistics or only for a specific interface.

Syntax

clear ipv6 dhcp statistics [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	(Optional) Specifies the interface for which to clear DHCPv6 statistics.

Defaults

If no interface is specified, IPv6 DHCP statistics for all interfaces are cleared.

Mode

Router privileged execution: C3(su)->router#

Example

This example clears DHCPv6 statistics for VLAN 80.

```
C3(su)->router# clear ipv6 dhcp statistics vlan 80
```

show ipv6 dhcp pool

This command displays information about a specific configured pool.

Syntax

show ipv6 dhcp pool *pool-name*

Parameters

pool-name	The name of the configured address pool for which to display information.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Usage

The information displayed by this command differs, depending on the configuration parameters of the pool.

Examples

This example displays the output for PoolA that was not configured for prefix delegation.

```
C3(su)->router# show ipv6 dhcp pool PoolA

DHCPv6 Pool: PoolA

DNS Server: 2001:db8:1234:5678::A
Domain Name: enterasys.com
```

This example displays the output for PoolB that was configured for prefix delegation.

```
C3(su)->router# show ipv6 dhcp pool PoolB

DHCPv6 Pool: PoolB
Client DUID: 00:02:00:00:00:11:0A:C0:89:D3:03:00:09:AA
Host:
Prefix/Prefix Length: 2001:db8:10::/48
Preferred Lifetime: 2592000
Valid Lifetime: 604800
DNS Server:
Domain Name:
```

show ipv6 dhcp binding

This command displays information about DHCPv6 bindings.

Syntax

show ipv6 dhcp binding [*ipv6-addr*]

Parameters

ipv6-addr	(Optional) Specifies the IPv6 address of the DHCP prefix delegation client for which to display binding information.

Defaults

If no IPv6 address is specified, all bindings are displayed.

Mode

Router privileged execution: C3(su)->router#

Example

This example displays all bindings for the client with the IPv6 address FE80::111:FCF1:DEA5:10.

```
C3(su)->router# show ipv6 dhcp binding FE80::111:FCF1:DEA5:10

DHCP Client Address: FE80::111:FCF1:DEA5:10
  DUID: 000300010002FCA5DC1C
  IA ID: 0x00040001, T1 0, T2 0
  Prefix/Prefix Length: 3FFE:C00:C18:11::/68
  Prefix Type: IPPD
  Expiration: 12320 seconds
  Valid Lifetime: 12345
  Preferred Lifetime: 180
```

25

OSPFv3 Configuration

*** IPv6 Routing License Required ***

IPv6 routing must be enabled with a license key in order to use this feature. If you have purchased an IPv6 routing license key, and have enabled routing on the device, you must activate your license as described in the chapter entitled “Activating Licensed Features” in order to enable the OSPFv3 protocol configuration command set. If you wish to purchase an IPv6 routing license, contact Enterasys Networks Sales.

The commands in this chapter perform configuration of the OSPFv3 routing protocol on the SecureStack C3. For information about general IPv6 configuration, refer to Chapter 22, **IPv6 Configuration**. For information about managing IPv6 host functionality at the switch level, refer to Chapter 21, **IPv6 Management**.

Overview

OSPFv3 is the Open Shortest Path First routing protocol for IPv6. It is similar to OSPFv2 in its concept of a link state database, intra/inter area and AS external routes and virtual links. OSPFv3 also differs from OSPFv2 in a number of respects:

- Peering is done via link-local addresses.
- The protocol is link- rather than network-centric.
- Addressing semantics have been moved to leaf LSAs, which eventually will allow its use for both IPv4 and IPv6.
- Two new LSAs have been introduced: the link LSA and the intra-area LSA.

Point-to-point links are supported in order to enable operation over tunnels. OSPFv3 views IPv6-over-IPv4 tunnels as a point-to-point interface with a link-local address and possibly, a global unicast address. OSPFv3 uses the reported MTU for tunnel interfaces.

OSPFv3 supports ECMP routes. OSPFv3 includes NSSA and AS-external LSA overflow limit support. RFC 1583 compatibility does not apply to OSPFv3. No OSPFv3 authentication methods are supported at this time.

LSA formats are changed, and the type 3 and 4 summary LSAs are renamed “inter-area-prefix” and “inter-area-router” LSAs. Also note that OSPFv3 LSA identifiers contain no addressing

semantics. LSA scope is generalized to link, area, and AS scope. OSPFv3 specifies the processing of unsupported LSAs. Unsupported LSAs are maintained in the database and flooded according to scope. In OSPFv3, routers with 100 or more interfaces generate more than one router LSA. A new link LSA has been created. Addresses in LSAs are specified as [prefix, prefix length].

Area ID and Router ID remain 32 bit identifiers. OSPFv3 identifies Neighbors by router ID instead of the interface address used in OSPFv2.

Note that both OSPFv3 and OSPFv2 can be enabled and run on the SecureStack C3.

Default Conditions

The following table lists the default OSPFv3 conditions.

Condition	Default Value
IPv6 OSPF	Disabled
IPv6 OSPF cost	10
IPv6 OSPF dead-interval	40 seconds
IPv6 OSPF hello-interval	10 seconds
IPv6 OSPF mtu-ignore	Enabled
IPv6 OSPF network	Broadcast
IPv6 OSPF priority	1
IPv6 OSPF retransmit-interval	4
IPv6 OSPF transmit-delay	1
Area stub no-summary	Enabled
Area virtual-link dead-interval	40
Area virtual-link hello-interval	10
Area virtual-link retransmit-interval	5
Area virtual-link transmit-delay	1
Default-information originate	Metric — unspecified Type — 2
Distance OSPF	Intra — 8 Inter — 10 Type-1 — 13 Type-2 — 50
Administrative mode of OSPF	Enabled
Exit-overflow-interval	0
External-lsdb-limit	-1
Maximum-paths	4
Redistribute	Metric — unspecified Type — 2 Tag — 0
Trapflags	Enabled

Global OSPFv3 Configuration Commands

Purpose

These commands are used to configure a router ID for the OSPFv3 router, to enter router OSPFv3 configuration mode, and to configure global OSPFv3 parameters.

Command

ipv6 router id

This command configures a 32-bit integer, entered in 32-bit dotted-quad notation, used to uniquely identify this OSPFv3 router.

Syntax

ipv6 router id *ip-address*

Parameters

ip-address	Specifies the ID of the OSPFv3 router, in 32-bit dotted-quad notation.

Defaults

None.

Mode

Router global configuration: C3(su)->router(Config)#

Usage

Use this command to configure the OSPFv3 router ID.

Example

This example illustrates configuring the OSPFv3 router ID as 2.2.2.2.

```
C3(su)->router(Config)# ipv6 router id 2.2.2.2
```

ipv6 router ospf

This command enters Router OSPFv3 configuration mode.

Syntax

ipv6 router ospf

Parameters

None.

Defaults

None.

Mode

Router global configuration: C3(su)->router(Config)#

Usage

Use this command to enter OSPFv3 configuration mode so you can configure global OSPFv3 parameters.

Example

This example illustrates entering router OSPFv3 configuration mode.

```
C3(su)->router(Config)# ipv6 router ospf
C3(su)->router(Config-router)#
```

default-information originate

This command is used to control the advertisement of default routes.

Syntax

default-information originate [**always**] [**metric** *value*] [**metric-type** *type*]

no default-information originate [**metric**] [**metric-type**]

Parameters

always	(Optional) Always advertises the default route information.
metric *value*	(Optional) Specifies the metric of the default route. The metric *value* can range from 0 to 16777214.
metric-type *type*	(Optional) Specifies the metric type of the default route. The metric *type* can be **1**, which specifies type 1 external route, or **2**, which specifies type 2 external route.

Defaults

A default external route is not generated.

The default metric is unspecified.

The default type is type 2.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Use this command to generate a default external route into an OSPFv3 routing domain. Use the **no** form of this command to stop the generation of a default external route.

Example

This example specifies a metric of 100 for the default route redistributed into the OSPFv3 routing domain, and an external metric type of 1.

```
C3(su)->router(Config-router)# default-information originate metric 100
metric-type 1
```

default-metric

This command sets a default metric for routes redistributed from another protocol into OSPFv3.

Syntax

default-metric *metric*

no default-metric

Parameters

metric	The value of *metric* can range from 1 to 16777214.

Defaults

No default metric is configured.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Use this command to cause the same metric value to be used for all redistributed routes.

Use the **no** form of this command to remove a configured default metric.

Example

This example configures a metric of 100 to be used for all redistributed routes.

```
C3(su)->router(Config-router)# default-metric 100
```

distance ospf

This command sets the route preference value of OSPFv3.

Syntax

distance ospf {**intra** | **inter** | **type1** | **type2**} *preference*

no distance ospf {**intra** | **inter** | **type1** | **type2**}

Parameters

intra	Specifies the preference for intra-area routes (all routes within an area)
inter	Specifies the preference for inter-area routes (all routes between areas)
type1	Specifies the preference for Type 1 external routes (routes learned by redistribution from other routing domains)
type2	Specifies the preference for Type 2external routes (routes learned by redistribution from other routing domains)
preference	The *preference* range is from 1 to 255.

Defaults

The default preference values are:

Intra-area = 8

Inter-area = 10

Type 1 = 13

Type 2 = 50

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Lower route preference values are preferred when determining the best route. The OSPFv3 specification (RFC 2328) requires that preferences must be given to the routes learned via OSPFv3 in the following order: intra-area < inter-area < Type 1 < Type 2.

A route with a preference of 255 cannot be used to forward traffic.

Use the **no** form of this command to reset the preference values back to the defaults.

Example

The following example set the intra-area preference to 5.

```
C3(su)->router(Config-router)# distance ospf intra 5
```

exit-overflow-interval

This command configures the exit overflow interval for OSPFv3.

Syntax

exit-overflow-interval *seconds*

no exit-overflow-interval

Parameters

seconds	Specifies the range for *seconds*, which is from 0 to 2147483647.

Defaults

The default interval value is 0.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

The exit overflow interval is the number of seconds after entering Overflow state that a router will wait before attempting to leave the Overflow State. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave Overflow State until restarted.

The **no** form of this command resets the interval to the default of 0.

Example

This example sets the exit overflow interval to 10 seconds.

```
C3(su)->router(Config-router)# exit-overflow-interval 10
```

external-lsdb-limit

This command configures the external LSDB limit for OSPFv3.

Syntax

external-lsdb-limit *limit*

no external-lsdb-limit

Parameters

limit	Specifies the *limit*, which can range from -1 to 2147483647. A value of -1 means that there is no limit.

Defaults

The default value is -1.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPFv3 backbone and/or any regular OSPFv3 area.

The **no** form of this command resets the limit to the default value of -1, meaning no limit.

Example

This example sets the external LSDB limit to 1000.

```
C3(su)->router(Config-router)# external-lsdb-limit 1000
```

maximum-paths

This command sets the number of paths that OSPFv3 can report for a given destination.

Syntax

maximum-paths *maxpaths*

no maximum-paths

Parameters

maxpaths	Specifies the value for *maxpaths*, which can range from 1 to 4.

Defaults

The default value is 4.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Use the **no** form of this command to reset the maximum number of paths to the default value of 4.

Example

This example sets the maximum number of paths for a given destination to 3.

```
C3(su)->router(Config-router)# maximum-paths 3
```

redistribute

This command configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.

Syntax

redistribute {**connected** | **static**} [**metric** *value*] [**metric-type** *type*] [**tag** *tag*]

no redistribute {**connected** | **static**} [**metric**] [**metric-type**] [**tag**]

Parameters

connected | **static**	Specifies the source protocol to redistribute.
metric *value*	(Optional) Specifies the route redistribution metric. The metric *value* can range from 0 to 16777214.
metric-type *type*	(Optional) Specifies the route redistribution metric type. The metric *type* can be **1**, which specifies type 1 external route, or **2**, which specifies type 2 external route.
tag *tag*	(Optional) Specifies a route redistribution tag. The value of *tag* can range from 0 to4294967295.

Defaults

The default values are:

Metric = unspecified

Metric type = Type 2

Tag = 0

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

The **no** form of this command configures the OSPFv3 protocol to prohibit redistribution of routes from the specified source protocol/routers.

Example

This example configures route redistribution of static routes and applies a metric of 10

```
C3(su)->router(Config-router)# redistribute static metric 10
```

Area Configuration Commands

Purpose

These commands are used to configure area parameters.

Commands

area default-cost

This command configures the default cost for the summary default route generated by the area border router into the stub or NSSA area.

Syntax

area *areaid* **default-cost** *cost*

no area *areaid* **default-cost**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.
cost	Specifies a *cost*, which can range between 1 and 16777215.

Defaults

None.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Use this command to set the cost value for the default route that is sent into a stub area or NSSA by an Area Border Router (ABR). The **no** form of this command removes the cost value from the summary route that is sent into the stub area.

Example

This example sets the default route cost to 50 for area 20.

```
C3(su)->router(Config-router)# area 20 default-cost 50
```

area nssa

This command configures the specified area to function as a not so stubby area (NSSA).

Syntax

area *areaid* **nssa**

no area *areaid* **nssa**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.

Defaults

None.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

An NSSA allows some external routes represented by external Link State Advertisements (LSAs) to be imported into it. This is in contrast to a stub area that does not allow any external routes. External routes that are not imported into an NSSA can be represented by means of a default route. This configuration is used when an OSPFv3 internetwork is connected to multiple non-OSPF routing domains.

The **no** form of this command changes the NSSA back to a plain area.

Example

This example shows how to configure area 20 as an NSSA.

```
C3(su)->router(Config-router)# area 20 nssa
```

area nssa default-info-originate

This command configures the metric value and type for the default route advertised into the NSSA.

Syntax

area *areaid* **nssa default-info-originate** [*metric*] [**comparable** | **non-comparable**]

no area *areaid* **nssa default-info-originate**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.
metric	(Optional) Specifies the metric of the default route, in the range of 1 to 16777214.
comparable | **non-comparable**	(Optional) Specifies the metric type: • **comparable** — nssa-external 1 • **non-comparable** — nssa-external 2

Defaults

Default metric value is 10.

Mode

Router OSPFv3 configuration: C3`(su)->router(Config-router)#`

Usage

Use this command to allow a default route to be advertised within the area. This option should be configured only on area border routers (ABRs).

Use the **no** form of this command to prevent a default route to be advertised within the area.

Example

This example configures NSSA area 20 to advertise a default route.

```
C3(su)->router(Config-router)# area 20 nssa default-info-originate
```

area nssa no-redistribute

This command configures the NSSA area border router to not redistribute learned external routes to the NSSA.

Syntax

area *areaid* **no-redistribute**

no area *areaid* **no-redistribute**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.

Defaults

None.

Mode

Router OSPFv3 configuration: C3`(su)->router(Config-router)#`

Usage

Use this command to prevent redistribution of learned external routes to the NSSA by this area border router (ABR). Use the **no** form of this command to enable redistribution of learned external routes to the NSSA.

Example

This example configures the router to not redistribute learned external routes into NSSA 20.

```
C3(su)->router(Config-router)# area 20 no-redistribute
```

area nssa no-summary

This command configures the NSSA area border router to not advertise summary routes into the NSSA.

Syntax

area *areaid* **nssa no-summary**

no area *areaid* **nssa no-summary**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.

Defaults

None.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Use this command to prevent the advertising of summary routes into the specified NSSA by this router. Use the **no** form of this command to enable advertising of summary routes into the NSSA.

Example

This example the router to not advertise summary routes into NSSA 20.

```
C3(su)->router(Config-router)# area 20 nssa no-summary
```

area nssa translator role

This command configures the translator role of the router.

Syntax

area *areaid* **nssa translator-role** {**always** | **candidate**}

no area *areaid* **nssa translator-role**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.
always	Specifies that the router will always assume the role of the translator the instant is becomes a border router.
candidate	Specifies that the router will participate in the translator election process when it becomes a border router.

Defaults

By default, the translator role is disabled.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

The NSSA Translator Role specifies whether or not an NSSA router will unconditionally translate Type-7 LSAs to Type-5 LSAs when acting as an NSSA border router.

When the **always** parameter is specified with this command, the router will always translate Type-7 LSAs, regardless of the translator state of other NSSA border routers. When the **candidate** parameter is specified, the NSSA router will participate in the translator election process described in RFC 3101, "The OSPF Not-So-Stubby Area (NSSA) Option."

Use the **no** form of this command to return the configured translator role to the default of disabled.

Example

This example configures the router to always assume the translator role when it becomes an area border router for NSSA 20.

```
C3(su)->router(Config-router)# area 20 nssa translator-role always
```

area nssa translator-stab-intv

This command configures the translator stability interval of the NSSA.

Syntax

area *areaid* **translator-stab-intv** *interval*

no area *areaid* **translator-stab-intv**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.
interval	Specifies the stability interval in seconds. The value of *interval* can range from 0 to 3600 seconds.

Defaults

The default interval is 40 seconds.

Mode

Router OSPFv3 configuration: C3`(su)->router(Config-router)#`

Usage

The stability interval is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Example

This example sets the translator stability interval to 60 seconds for NSSA 20.

```
C3(su)->router(Config-router)# area 20 nssa translator-stab-intv 60
```

area range

This command creates an address range for the specified NSSA.

Syntax

area *areaid* **range** *ipv6-prefix/prefix-length* {**summarylink** | **nssaexternallink**} [**advertise** | **not-advertise**]

no area *areaid* **range** *ipv6-prefix/prefix-length*

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.
ipv6-prefix/prefix-length	Specifies IPv6 prefix and the length of the IPv6 prefix for the address range. The prefix must be specified in hexadecimal using 16-bit values between colons. The value of *prefix-length* is a decimal number indicating the number of high-order contiguous bits that comprise the prefix.
summarylink	Specifies that route summarization should be based on summary LSAs.
nssaexternallink	Specifies that route summarization should be based on external LSAs Type 7.
advertise | **not-advertise**	(Optional) Specifies whether or not the routes should be advertised. If neither parameter is specifies, the default is **advertise**.

Defaults

Area address ranges are not configured by default.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Address ranges control the advertisement of routes across area boundaries. Routing information is summarized, or aggregated, at area boundaries. External to the area, at most a single route is advertised (via an inter-area-prefix-LSA) for each address range. A route is advertised if and only if the address range's status is set to **advertise**. The default condition is to advertise.

For ABRs configured for NSSA, route summarization/aggregation can be implemented based on LSA type — either summary LSAs (specified with the **summarylink** parameter), or NSSA external LSAs Type 7 (specified with the **nssaexternallink** parameter).

You can configure multiple address ranges with this command.

Use the **no** form of this command to remove a configured address range.

Example

This example configures an address range to be consolidated and advertised based on summary LSAs.

```
C3(su)->router(Config-router)# area 20 range 3FFe:501::/32 summarylink
```

area stub

This command creates a stub area for the specified area ID.

Syntax

area *areaid* **stub**

no area *areaid* **stub**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.

Defaults

None.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

A stub area is characterized by the fact that AS external LSAs are not propagated into the area. Removing AS external LSAs and summary LSAs can significantly reduce the link state database of routers within the stub area.

Use the **no** form of the command to delete a stub area.

Example

This example creates a stub area with the ID of 30.

```
C3(su)->router(Config-router)# area 30 stub
```

area stub no-summary

This command disables the import of summary LSAs into the specified stub area.

Syntax

area *areaid* **stub no-summary**

no area *areaid* **stub no-summary**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.

Defaults

None.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Use the no form of this command to set the summary LSA import mode to the default for the specified stub area.

Example

The example disables the import of summary LSAs into stub area 30.

```
C3(su)->router(Config-router)# area 30 stub no-summary
```

area virtual-link

This command creates the OSPFv3 virtual interface for the specified area and neighbor.

Syntax

area *areaid* **virtual-link** *neighborid*

no area *areaid* **virtual-link** *neighborid*

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.
neighborid	Specifies the virtual link neighbor by means of its router ID. The router ID must be entered in 32-bit dotted-quad notation.

Defaults

None.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

The virtual link neighbor is identified by its router ID. Use the **no** form of this command to delete the configured OSPFv3 virtual interface identified by area and neighbor.

Example

This example creates a virtual interface for area 20 and the neighbor with router ID 2.2.2.2.

```
C3(su)->router(Config-router)# area 20 virtual-link 2.2.2.2
```

area virtual-link dead-interval

This command configures the dead interval for the specified OSPFv3 virtual interface.

Syntax

area *areaid* **virtual-link** *neighborid* **dead-interval** *seconds*

no area *areaid* **virtual-link** *neighborid* **dead-interval**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.
neighborid	Specifies the virtual link neighbor by means of its router ID. The router ID must be entered in 32-bit dotted-quad notation.
seconds	Specifies the value of the dead interval in seconds. The range is from 1 to 65535 seconds.

Defaults

The default dead interval is 40 seconds.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Use the no form of this command to return a configured value to the default of 40 seconds.

Example

This example configures a dead interval of 60 seconds for the specified virtual interface.

```
C3(su)->router(Config-router)# area 20 virtual-link 2.2.2.2 dead-interval 60
```

area virtual-link hello-interval

This command configures the hello interval for the specified OSPFv3 virtual interface.

Syntax

area *areaid* **virtual-link** *neighborid* **hello-interval** *seconds*

no area *areaid* **virtual-link** *neighborid* **hello-interval**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.
neighborid	Specifies the virtual link neighbor by means of its router ID. The router ID must be entered in 32-bit dotted-quad notation.
seconds	Specifies the value of the hello interval in seconds. The range is from 1 to 65535 seconds.

Defaults

The default hello interval is 10 seconds.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Use the **no** form of this command to return a configured value to the default value of 10 seconds.

Example

This example configures a hello interval of 30 seconds for the specified OSPFv3 virtual interface.

```
C3(su)->router(Config-router)# area 20 virtual-link 2.2.2.2 hello-interval 30
```

area virtual-link retransmit-interval

This command configures the retransmit interval for the specified OSPFv3 virtual interface.

Syntax

area *areaid* **virtual-link** *neighborid* **retransmit-interval** *seconds*

no area *areaid* **virtual-link** *neighborid* **retransmit-interval**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.
neighborid	Specifies the virtual link neighbor by means of its router ID. The router ID must be entered in 32-bit dotted-quad notation.
seconds	Specifies the value of the retransmit interval in seconds. The range is from 1 to 3600 seconds.

Defaults

The default retransmit interval is 5 seconds.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Use the **no** form of this command to return a configured value to the default value of 5 seconds.

Example

This example sets the retransmit interval to 10 seconds for the specified OSPFv3 virtual interface.

```
C3(su)->router(Config-router)# area 20 virtual-link 2.2.2.2 retransmit-interval
10
```

area virtual-link transmit-delay

This command configures the transmit delay for the specified OSPFv3 virtual interface.

Syntax

area *areaid* **virtual-link** *neighborid* **transmit-delay** *seconds*

no area *areaid* **virtual-link** *neighborid* **transmit-delay**

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.
neighborid	Specifies the virtual link neighbor by means of its router ID. The router ID must be entered in 32-bit dotted-quad notation.
seconds	Specifies the value of the transmit delay in seconds. The range is from 1 to 3600 seconds.

Defaults

The default transmit delay is 1 second.

Mode

Router OSPFv3 configuration: C3(su)->router(Config-router)#

Usage

Use the **no** form of this command to reset the transmit delay to the default of 1 second.

Example

This example sets the transmit delay to 2 seconds for the specified OSPFv3 virtual interface.

```
C3(su)->router(Config-router)# area 20 virtual-link 2.2.2.2 transmit-delay 2
```

Interface Configuration Commands

Purpose

These commands can be used to configure OSPF v3 routing interface parameters.

Commands

ipv6 ospf enable

This command enables OSPFv3 on a router interface or a loopback interface.

Syntax

```
ipv6 ospf enable
no ipv6 ospf enable
```

Parameters

None.

Defaults

OSPFv3 is disabled by default.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

Use this command to enable OSPFv3 on a router VLAN interface or on a loopback interface. Use the **no** form of this command to disable OSPFv3 on an interface.

Note: In order for OSPFv3 to run on an interface, IPv6 must be explicitly enabled on the interface using the **ipv6 enable** command.

Example

This example enters router interface configuration mode for VLAN 7 and then enables OSPFv3 on the interface.

```
C3(su)->router(Config)# interface vlan 7
C3(su)->router(Config-if(Vlan 7))# ipv6 ospf enable
```

ipv6 ospf areaid

This command sets the OSPFv3 area to which the router interface belongs.

Syntax

ipv6 ospf areaid *areaid*

no ipv6 ospf areaid *areaid*

Parameters

areaid	Specifies the area ID in either 32-bit dotted-quad format or as a decimal number between 0 and 4294967295.

Defaults

None.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

The area ID uniquely identifies the area to which the interface connects. Assigning an area ID which does not exist on an interface causes the area to be created with default values.

Use the **no** form of this command to remove an area from the interface.

Examples

This example assigns VLAN 7 to area 20, expressed in dotted-quad format.

```
C3(su)->router(Config)# interface vlan 7
C3(su)->router(Config-if(Vlan 7))# ipv6 ospf areaid 0.0.0.20
```

This example assigns VLAN 7 to area 20, expressed as a decimal number.

```
C3(su)->router(Config-if(Vlan 7))# ipv6 ospf areaid 20
```

ipv6 ospf cost

This command configures the cost of sending a packet on an OSPFv3 interface.

Syntax

ipv6 ospf cost *cost*

no ipv6 ospf cost *cost*

Parameters

cost	Specifies the cost of sending a packet on this interface. The value can range from 1 to 65535.

Defaults

The default cost is 10.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

Use this command to explicitly specify the cost of sending a packet on the interface being configured for OSPFv3. Use the **no** form of this command to return the cost to the default value of 10.

Example

This example configures the cost for router interface VLAN 7 to 100.

```
C3(su)->router(Config)# interface vlan 7
C3(su)->router(Config-if(Vlan 7))# ipv6 ospf cost 100
```

ipv6 ospf dead-interval

This command sets the OSPFv3 dead interval for the router interface.

Syntax

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval *seconds*

Parameters

seconds	Specifies the OSPFv3 dead interval in seconds. The value can range from 1 to 2147483647 seconds.

Defaults

The default dead interval value is 40 seconds.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

The OSPFv3 dead interval is the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the dead interval must be the same for all routers attached to a common network, and should be some multiple of the hello interval.

Use the **no** form of this command to return the dead interval to the default value of 40 seconds.

Example

This example sets the dead interval for router interface VLAN 7 to 60 seconds.

```
C3(su)->router(Config)# interface vlan 7
C3(su)->router(Config-if(Vlan 7))# ipv6 ospf dead-interval 60
```

ipv6 ospf hello-interval

This command sets the OSPFv3 hello interval for the router interface.

Syntax

ipv6 ospf hello-interval *seconds*

no ipv6 ospf hello-interval *seconds*

Parameters

seconds	Specifies the OSPFv3 hello interval in seconds. The value can range from 1 to 65535 seconds.

Defaults

The default hello interval is 10 seconds.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

Use this command to specify the interval between hello packets that OSPFv3 sends on the interface being configured. The shorter the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. The hello interval must be the same for all routers attached to a common network.

Use the **no** form of this command to return the hello interval to the default value of 10 seconds.

Example

This example sets the hello interval for router interface VLAN 7 to 20 seconds.

```
C3(su)->router(Config)# interface vlan 7
C3(su)->router(Config-if(Vlan 7))# ipv6 ospf hello-interval 20
```

ipv6 ospf mtu-ignore

This command disables OSPFv3 maximum transmission unit (MTU) mismatch detection.

Syntax

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Parameters

None.

Defaults

By default, MTU mismatch detection is enabled.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Use this command to prevent the OSPFv3 router process from checking whether neighbors are using the same maximum transmission unit (MTU) on a common interface when exchanging Database Description packets.

Use the **no** form of this command to enable MTU mismatch detection.

Example

This example disables MTU mismatch detection on router interface VLAN 7.

```
C3(su)->router(Config)# interface vlan 7
C3(su)->router(Config-if(Vlan 7))# ipv6 ospf mtu-ignore
```

ipv6 ospf network

This command changes the default OSPFv3 network type for the router interface.

Syntax

```
ipv6 ospf network {broadcast | point-to-point}
no ipv6 ospf network {broadcast | point-to-point}
```

Parameters

broadcast	Sets the network type to broadcast.
point-to-point	Sets the network type to point-to-point.

Defaults

Default network type is broadcast.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

Normally, the network type is determined from the physical IP network type. By default, all Ethernet networks are OSPFv3 type broadcast. Similarly, tunnel interfaces default to point-to-point. When an Ethernet port is used as a single large bandwidth IP network between two routers, the network type can be point-to-point since there are only two routers. Using point-to-point as the network type eliminates the overhead of the OSPFv3 designated router election. It is normally not useful to set a tunnel to OSPFv3 network type broadcast.

Use the **no** form of this command to set the network type to the default.

Example

This example sets the network type to point-to-point for router interface VLAN 7.

```
C3(su)->router(Config)# interface vlan 7
C3(su)->router(Config-if(Vlan 7))# ipv6 ospf network point-to-point
```

ipv6 ospf priority

This command sets the OSPFv3 priority for the router interface. Router priority helps determine the designated router for an OSPFv3 link.

Syntax

ipv6 ospf priority *priority*

no ipv6 ospf priority

Parameters

priority	Specifies the priority value, which can range from 0 to 255.

Defaults

Default priority value is 1.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

When two routers on the same network attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router.

Use the **no** form of this command to return priority value to the default of 1.

Example

This example sets the priority for router interface VLAN 7 to 5.

```
C3(su)->router(Config)# interface vlan 7
C3(su)->router(Config-if(Vlan 7))# ipv6 ospf priority 5
```

ipv6 ospf retransmit-interval

This command configures the OSPFv3 retransmit interval for the router interface.

Syntax

ipv6 ospf retransmit-interval *seconds*

no ipv6 ospf retransmit-interval

Parameters

seconds	Specifies the retransmit interval value, which can range from 0 to 3600 seconds.

Defaults

Default value is 4 seconds.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

The retransmit interval is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets.

Use the **no** form of this command to reset the retransmit interval to the default value of 4 seconds.

Example

This example sets the retransmit interval to 10 seconds for router interface VLAN 7.

```
C3(su)->router(Config)# interface vlan 7
C3(su)->router(Config-if(Vlan 7))# ipv6 ospf retransmit-interval 10
```

ipv6 ospf transmit-delay

This command sets the OSPFv3 transmit delay for the router interface.

Syntax

ipv6 ospf transmit-delay *seconds*

no ipv6 ospf transmit-delay

Parameters

seconds	Specifies the transmit delay, which can range from 1 to 3600 seconds.

Defaults

Default value is 1 second.

Mode

Router interface configuration: C3(su)->router(Config-if(Vlan 1))#

Usage

The transmit delay, specified in seconds, sets the estimated number of seconds it takes to transmit a link state update packet over this interface.

Use the **no** form of this command to return the transmit delay to the default value of 1 seconds.

Example

This example sets the transmit delay value to 4 seconds for router interface VLAN 7.

```
C3(su)->router(Config)# interface vlan 7
C3(su)->router(Config-if(Vlan 7))# ipv6 ospf transmit-delay 4
```

OSPFv3 Show Commands

Purpose

These commands are used to display OSPFv3 information and statistics.

Commands

show ipv6 ospf

This command displays OSPFv3 router information.

Syntax

`show ipv6 ospf`

Parameters

None.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Example

This example shows how to display OSPFv3 router information.

```
C3(su)->router# show ipv6 ospf
Router ID                                       2.2.2.2
OSPF Admin Mode                                 Enable
ASBR Mode                                       Enable
```

```
ABR Status                                    Enable
Exit Overflow Interval                        0
External LSA Count                            0
External LSA Checksum                         0
New LSAs Originated                           89
LSAs Received                                 177
External LSDB Limit                           No Limit
Default Metric                                Not Configured
Maximum Paths                                 4
Default Route Advertise                       Disabled
Always                                        FALSE
Metric
Metric Type                                   External Type 2
```

Table 25-1 provides an explanation of the command output.

Note: Some of the information in Table 25-1 displays only if you enable OSPFv3 and configure certain features.

Table 25-1 show ipv6 ospf Output Details

Output Field	What It Displays...
Router ID	A 32 bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.
OSPF Admin Mode	Whether the administrative mode of OSPF in the router is enabled or disabled. This is a configured value.
ASBR Mode	Whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learnt by other protocols) or disabled (if the router is not configured for the same).
ABR Status	Whether the router is an OSPF Area Border Router.
Exit Overflow Interval	The number of seconds that, after entering Overflow State, a router will attempt to leave Overflow State.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
External LSA Checksum	The sum of the LS checksums of external link-state advertisements contained in the link-state database.
New LSAs Originated	The number of new link-state advertisements that have been originated.
LSAs Received	The number of link-state advertisements received determined to be new instantiations.
External LSDB Limit	The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.
Default Metric	Default value for redistributed routes.
Maximum Paths	The maximum number of paths that OSPF can report for a given destination.
Default Route Advertise	Whether the default routes received from other source protocols are advertised or not.

Table 25-1 show ipv6 ospf Output Details

Output Field	What It Displays...
Always	Whether default routes are always advertised.
Metric	The metric for the advertised default routes. If the metric is not configured, this field is blank.
Metric Type	Whether the routes are External Type 1 or External Type 2.

show ipv6 ospf area

This command displays information about the specified OSPFv3 area.

Syntax

show ipv6 ospf area *areaid*

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Example

This example shows how to display OSPFv3 information for area 20.

```
C3(su)->router>show ipv6 ospf area 20
AreaID                                      0.0.0.20
External Routing                            Import NSSAs
Spf Runs                                    7
Area Border Router Count                    0
Area LSA Count                              5
Area LSA Checksum                           188094
Stub Mode                                   Disable
```

Table 25-2 provides an explanation of the command output.

Table 25-2 show ipv6 ospf area Output Details

Output Field	What It Displays...
AreaID	Area ID of the requested OSPFv3 area.
External Routing	The external routing capabilities for this area.
Spf Runs	Number of times that the intra-area route table has been calculated using this area's link-state database.
Area Border Router Count	Total number of area border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.

Table 25-2 show ipv6 ospf area Output Details (Continued)

Output Field	What It Displays...
Area LSA Checksum	Number representing the Area LSA Checksum for the specified Area ID excluding the external (LS type 5) link-state advertisements.
Stub Mode	Whether the specified area is a stub area or not. The possible values are enabled and disabled. This is a configured value.
Import Summary LSAs	Whether to import summary LSAs (enabled or disabled).
OSPF Stub Metric Value	Metric value of the stub area. This field displays only if the area is a configured as a stub area.

show ipv6 ospf abr

This command displays OSPFv3 routes to reach area border routers.

Syntax

```
show ipv6 ospf abr
```

Parameters

None.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Example

This example shows how to display OSPFv3 area border router information.

```
C3(su)->router# show ipv6 ospf abr
Type    Router Id    Cost   Area ID             Next Hop               Next Hop
                                                                       Intf
----- -------------- ---- ----------- -------------------------------- --------
INTRA 82.15.0.1      10   0.0.0.10     FE80::200:2DFF:FEE6:FB6B         Vlan 48
```

Table 25-3 provides an explanation of the command output.

Table 25-3 show ipv6 ospf abr Output Details

Output Field	What It Displays...
Type	The type of the route to the destination, which is one of the following values: INTRA — Intra-area route INTER — Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.

Table 25-3 show ipv6 ospf abr Output Details (Continued)

Output Field	What It Displays...
Next Hop Intf	Address of the next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

show ipv6 ospf asbr

This command displays OSPFv3 routes to reach AS border routers.

Syntax

```
show ipv6 ospf asbr
```

Parameters

None.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Example

This example shows how to display OSPFv3 AS border router routes.

```
C3(su)->router# show ipv6 ospf asbr

Type    Router Id    Cost   Area ID              Next Hop                Next Hop
                                                                         Intf
----- -------------- ---- ------------ -------------------------------- --------
INTER 1.11.1.1       5    0.0.0.20     FE80::100:1111:FEE6:FB7A         Vlan 35
```

Table 25-4 provides an explanation of the command output.

Table 25-4 show ipv6 ospf asbr Output Details

Output Field	What It Displays...
Type	The type of the route to the destination, which is one of the following values: INTRA — Intra-area route INTER — Inter-area route
Router ID	Router ID of the destination.
Cost	Cost of using this route.
Area ID	The area ID of the area from which this route is learned.
Next Hop	Address of the next hop toward the destination.
Next Hop Intf	The outgoing router interface to use when forwarding traffic to the next hop.

show ipv6 ospf database

This command displays information about the link state database when OSPFv3 is enabled.

Syntax

```
show ipv6 ospf [areaid] database [{external | inter-area {prefix | router} | link |
network | nssa-external | prefix | router | unknown {area | as | link}}]
[lsid] [{adv-router [rtrid] | self-originate | database-summary}]
```

Parameters

areaid	(Optional) Display database information about a specific area. Enter the area ID in IP address format (dotted-quad) or as a decimal value.
external	(Optional) Display external LSAs.
inter-area	(Optional) Display inter-area LSAs.
prefix	(Optional) Display intra-area Prefix LSAs.
router	(Optional) Display router LSAs.
link	(Optional) Display link LSAs.
network	(Optional) Display network LSAs.
nssa-external	(Optional) Display NSSA external LSAs.
unknown {**area** | **as** | **link**}	(Optional) Display unknown area, unknown AS, or unknown link LSAs.
lsid	(Optional) Specifies the link state ID.
adv-router [*rtrid*]	(Optional) Display the LSAs that are restricted by the advertising router. Optionally, specify the router by its router ID (*rtrid*), entered as a 32-bit dotted-quad value.
self-originate	(Optional) Display LSAs that are self-originated.
database-summary	(Optional) Displays the number of each type of LSA in the database and the total number of LSAs in the database.

Defaults

If no parameters are entered, LSA headers for all areas are displayed.

Mode

Router privileged execution: C3(su)->router#

Usage

If you execute this command without any parameters, LSA headers for all areas are displayed. Use the *areaid* parameter to display database information for a specific area. The other optional parameters can be used to specify a particular type of link state advertisement to display.

Examples

This example displays the output when an area ID is specified.

```
C3(su)->router#show ipv6 ospf 10 database

                Inter Network States (Area 0.0.0.10)
```

```
Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
2.2.2.2                       1 153   80000026 A8F2

                Intra Prefix  States (Area 0.0.0.10)

Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
2.2.2.2                       0 506   80000027 DD00

                 AS External States

Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
2.2.2.2                       1 342   8000002C 0C20
```

This example shows partial output of this command when no parameters are specified.

```
C3(su)->router>show ipv6 ospf database

                router links States (Area 0.0.0.0)

Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
2.2.2.2                       0 1288   80000273 32A9 V6E--R- ---EB
3.3.3.3                       0 1098   80000251 7D11 V6E--RD -----

                network links States (Area 0.0.0.0)

Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
3.3.3.3                       3 1098   800001DB 8A7F V6E--RD

                Link States (Area 0.0.0.0)

Adv Router      Link Id         Age   Sequence Csum Options Rtr Opt
--------------- --------------- ----- -------- ---- ------- -------
3.3.3.3                       3 1098   800001DA 0F95 V6E--RD
2.2.2.2                     426 1288   80000213 DFC0 V6E--R-
--More-- or (q)uit
```

This example illustrates the output of this command using the **adv-router** parameter.

```
C3(su)->router>show ipv6 ospf database external adv-router

                AS External States

LS Age: 930
LS Type: AS-External-LSA
LS Id: 1
Advertising Router: 2.2.2.2
LS Seq Number: 0x80000006
Checksum: 0x3e4c
Length: 36
Options:(E-Bit)
```

```
Metric Type: 2
Metric:20
IPv6 Prefix: 2301::/64 (None)
```

Table 25-5 provides an explanation of the command output.

Table 25-5 show ipv6 ospf database Output Details

Output Field	What It Displays...
Link Id	Number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.
Advertising Router	The Advertising Router. Is a 32 bit dotted decimal number representing the LSDB interface.
LS Age	Number representing the age of the link state advertisement in seconds.
LS Type	The format and function of the specified LSA.
LS Seq Number	Number that represents which LSA is more recent.
Checksum	Total number LSA checksum.
Lenght	Size of the LSA in bytes.
Options	Option bits in LSA header. Refer to section A.2 in RFC 2740 for more information. Possible values are: V6 — indicates status of V6 bit. If this bit is clear, the router/link should be excluded from IPv6 routing calculations. E — indicates status of E-bit. This bit describes the way AS-external-LSAs are flooded. M — indicates the status of MC-bit. This bit describes whether IP multicast datagrams are forwarded. N — indicates the status of N-bit. This bit describes the handling of Type-7 LSAs. R — indicates the status of R-bit. This bit (the `Router' bit) indicates whether the originator is an active router. D — indicates the status of DC-bit. This bit describes the router's handling of demand circuits.
Metric Type	Whether the route specified is external type 1 or external type 2.
Metric	The cost of using the specified router link.
IPv6 Prefix	The IPv6 route with prefix mask being displayed.

This example shows how to display OSPF database summary information.

```
C3(su)->router#show ipv6 ospf database database-summary

OSPF Router with ID (2.2.2.2)


Area 0.0.0.0 Database Summary
Router                                          2
Network                                         1
Inter-area Prefix                               1
Inter-area Router                               0
Type-7 Ext                                      0
Link                                            2
```

```
Intra-area Prefix                          2
Link Unknown                               0
Area Unknown                               0
AS Unknown                                 0
AS Unknown                                 0
Self Originated Type-7                     0
Subtotal                                   8

Area 0.0.0.10 Database Summary
Router                                     2
Network                                    1
Inter-area Prefix                          51
Inter-area Router                          0
Type-7 Ext                                 0
Link                                       2
Intra-area Prefix                          2
Link Unknown                               0
Area Unknown                               0
AS Unknown                                 0
AS Unknown                                 0
Self Originated Type-7                     0
Subtotal                                   58


Router database summary
Router                                     4
Network                                    2
Inter-area Prefix                          52
Inter-area Router                          0
Type-7 Ext                                 0
Link                                       4
Intra-area Prefix                          4
Link Unknown                               0
Area Unknown                               0
AS Unknown                                 0
Type-5 Ext                                 0
Self-Originated Type-5 Ext                 0
Total                                      66
```

Table 25-6 provides an explanation of the **database-summary** command output.

Table 25-6 show ipv6 ospf database database-summary Output Details

Output Field	What It Displays...
Router	Total number of router LSAs in the OSPFv3 link state database.
Network	Total number of network LSAs in the OSPFv3 link state database.
Inter-area Prefix	Total number of inter-area prefix LSAs in the OSPFv3 link state database.
Inter-area Router	Total number of inter-area router LSAs in the OSPFv3 link state database.
Type-7 Ext	Total number of NSSA external LSAs in the OSPFv3 link state database.
Link	Total number of link LSAs in the OSPFv3 link state database.
Intra-area Prefix	Total number of intra-area prefix LSAs in the OSPFv3 link state database.

Table 25-6 show ipv6 ospf database database-summary Output Details (Continued)

Output Field	What It Displays...
Link Unknown	Total number of link-source unknown LSAs in the OSPFv3 link state database.
Area Unknown	Total number of area unknown LSAs in the OSPFv3 link state database.
AS Unknown	Total number of as unknown LSAs in the OSPFv3 link state database.
Self Originated Type-7	Total number of self-originated NSSA External Link-State Advertisements in the OSPFv3 link state database.
Type-5 Ext	Total number of AS external LSAs in the OSPFv3 link state database.
Self-Originated Type-5	Total number of self originated AS external LSAs in the OSPFv3 link state database.
Total	Total number of router LSAs in the OSPFv3 link state database.

show ipv6 ospf interface

This command displays information about OSPFv3 interfaces.

Syntax

show ipv6 ospf interface {**vlan** *vlanid* | **tunnel** *tunnelid* | **loopback** *loopid*}

Parameters

vlan *vlanid*	Specifies the VLAN interface to display information about.
tunnel *tunnelid*	Specifies the tunnel interface to display information about.
loopback *loopid*	Specifies the loopback interface to display information about.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Examples

This example displays information about OSPFv3 routing interface VLAN 80.

```
C3(su)->router>show ipv6 ospf interface vlan 80
IPv6 Address                                    FE80::211:88FF:FE56:5D8F
ifIndex                                         430
OSPF Admin Mode                                 Enable
OSPF Area ID                                    0.0.0.20
Router Priority                                 1
Retransmit Interval                             5
Hello Interval                                  10
Dead Interval                                   40
LSA Ack Interval                                1
Iftransit Delay Interval                        1
```

```
Authentication Type                             None
Metric Cost                                     10  (computed)
OSPF Mtu-ignore                                 Disable
OSPF Interface Type                             broadcast
State                                           designated-router
Designated Router                               2.2.2.2
Backup Designated Router                        0.0.0.0
Number of Link Events                           2
```

This example displays information about tunnel interface 0. Table 25-7 on page 25-39 explains the content of the output fields.

```
C3(su)->router#show ipv6 ospf interface tunnel 0
IPv6 Address                                    FE80::5000:2
ifIndex                                         456
OSPF Admin Mode                                 Enable
OSPF Area ID                                    0.0.0.0
Router Priority                                 1
Retransmit Interval                             5
Hello Interval                                  10
Dead Interval                                   40
LSA Ack Interval                                1
Iftransit Delay Interval                        1
Authentication Type                             None
Metric Cost                                     1  (computed)
OSPF Mtu-ignore                                 Disable
OSPF Interface Type                             point-to-point
State                                           point-to-point
Designated Router                               0.0.0.0
Backup Designated Router                        0.0.0.0
Number of Link Events                           1
```

Table 25-7 provides an explanation of the command output.

Table 25-7 show ipv6 ospf interface Command Output Details

Output Field	What It Displays...
IPv6 Address	The IPv6 address of the interface.
ifIndex	The interface index number associated with the interface.
OSPF Admin Mode	Whether the admin mode is enabled or disabled.
OSPF Area ID	The area ID associated with this interface.
Router Priority	The router priority. The router priority determines which router is the designated router.
Retransmit Interval	The frequency, in seconds, at which the interface sends LSA.
Hello Interval	The frequency, in seconds, at which the interface sends Hello packets.
Dead Interval	The amount of time, in seconds, the interface waits before assuming a neighbor is down.
LSA Ack Interval	The amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.
Iftransit Delay Interval	The number of seconds the interface adds to the age of LSA packets before transmission.
Authentication Type	The type of authentication the interface performs on LSAs it receives.

Table 25-7 show ipv6 ospf interface Command Output Details (Continued)

Output Field	What It Displays...
Metric Cost	The priority of the path. Low costs have a higher priority than high costs.
OSPF MTU-ignore	Whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers. The following information only displays if OSPF is initialized on the interface:
OSPF Interface Type	Broadcast LANs, such as Ethernet and IEEE 802.5, take the value broadcast. Tunnel interfaces take the value point-to-point.
State	The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.
Designated Router	The router ID representing the designated router.
Backup Designated Router	The router ID representing the backup designated router.
Number of Link Events	The number of link events.

show ipv6 ospf interface stats

This command displays statistics for a specific interface. Statistics are displayed only if OSPFv3 is enabled.

Syntax

show ipv6 ospf interface stats vlan *vlanid*

Parameters

vlan *vlanid*	Specifies the VLAN interface for which to display statistics.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Example

This example shows how to display statistics for VLAN 80.

```
C3(su)->router>show ipv6 ospf interface stats vlan 80
OSPFv3 Area ID                                  0.0.0.20
Spf Runs                                        7
Area Border Router Count                        0
AS Border Router Count                          0
Area LSA Count                                  5
IPv6 Address                                    FE80::211:88FF:FE56:5D8F/128
OSPF Interface Events                           2
Virtual Events                                  0
Neighbor Events                                 0
External LSA Count                              1
LSAs Received                                   1903
Originate New LSAs                              4198
Sent Packets                                    1053
```

```
Received Packets                              0
Discards                                      0
Bad Version                                   0
Virtual Link Not Found                        0
Area Mismatch                                 0
Invalid Destination Address                   0
No Neighbor at Source Address                 0
Invalid OSPF Packet Type                      0

  Packet Type           Sent      Received
--------------------  ----------  ----------
Hello                       1053           0
Database Description           0           0
LS Request                     0           0
LS Update                      0           0
LS Acknowledgement             0           0
```

Table 25-8 provides an explanation of the command output.

Table 25-8 show ipv6 ospf interface stats Output Details

Output Field	What It Displays...
OSPFv3 Area ID	The area ID of this OSPFv3 interface.
Spf Runs	Is the number of times that the intra-area route table has been calculated using this area's link-state database.
Area Border Router Count	The total number of area border routers reachable within this area.
AS Border Router Count	The total number of AS border routers reachable within this area.
Area LSA Count	Total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
IPv6 Address	The IP address associated with this OSPFv3 interface.
OSPF Interface Events	The number of times the specified OSPFv3 interface has changed its state, or an error has occurred.
Virtual Events	The number of state changes or errors that occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship has changed state, or an error has occurred.
External LSA Count	Total number of AS External link-state advertisements in this area's link-state database.
LSAs Received	Number of link-state advertisements received.
Originate New LSAs	Number of LSAs originated.
Sent Packets	The number of OSPFv3 packets sent on the interface.
Received Packets	The number of OSPFv3 packets received on the interface.
Discards	Number of packets discarded.
Bad Version	Number of bad version packets received.
Virtual Link Not Found	Number of virtual link not found packets received.
Area Mismatch	Number of area mismatch packets received.
Invalid Destination Address	Number of invalid destination address packets received.
No Neighbor at Source Address	Number of no neighbor at source address packets received.

Table 25-8 show ipv6 ospf interface stats Output Details

Output Field	What It Displays...
Invalid OSPF Packet Type	Number of packets received with invalid packet type.
Packet Type / Sent / Received	Columns listing packet types and number of packets sent and received per type.

show ipv6 ospf neighbor

This command displays information about OSPFv3 neighbors.

Syntax

show ipv6 ospf neighbor [**interface** {**vlan** *vlanid* | **tunnel** *tunnelid*}] [*neighborid*]

Parameters

interface	(Optional) Restricts the output display to a specific interface.
vlan *vlanid*	Specify the VLAN interface to display information about.
tunnel *tunnelid*	Specify the tunnel interface to display
neighborid	(Optional) Specify the neighbor by its router ID, specified in 32-bit dotted quad format.

Defaults

When no parameters are specified, information about all neighbors is displayed.

Mode

Router privileged execution: C3(su)->router#

Usage

If you do not specify a neighbor router ID, the output displays summary information in a table. If you specify an interface or tunnel, only the information for that interface or tunnel displays.

When you specify a neighbor by router ID, detailed information about the neighbor displays.

The information is displayed only if OSPFv3 is enabled and the interface has a neighbor.

Examples

This example illustrates the summary information displayed when no neighbor is specified.

```
C3(su)->router#show ipv6 ospf neighbor

   Router ID      Priority  Intf   Interface    State             Dead
                            ID                                    Time
---------------  --------  -----  -----------  ----------------  ----
3.3.3.3          1         3      Vlan 36      Full/DR           32
6.6.6.6          1         456    Tunnel 0     Full/PtP          31
```

Table 25-9 provides an explanation of the command output.

Table 25-9 show ipv6 ospf neighbor Output Details

Output Field	What It Displays...
Router ID	The 4-digit dotted-decimal number of the neighbor router.
Priority	OSPFv3 priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.
Intf ID	Interface ID of the neighbor.
Interface	Interface of the local router.
State	State of the neighboring routers. Possible values are: • Down- initial state of the neighbor conversation - no recent information has been received from the neighbor. • Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor. • Init - a Hello packet has recently been seen from the neighbor, but bidirectional communication has not yet been established. • 2 way - communication between the two routers is bidirectional. This is the final state between two routers, both of which are non-designated routers or back-up designated routers. • Exchange start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number. • Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor. • Loading - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state. • Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.
Dead Time	Amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

This example displays the output of this command when a neighbor is specified.

```
C3(su)->router#show ipv6 ospf neighbor 8.8.8.8

Interface                                   Vlan 45
Area Id                                     0.0.0.30
Options                                     0x2
Router Priority                             128
Dead timer due in (secs)                    33
State                                       Full/DR
Events                                      6
Retransmission Queue Length                 0
```

Table 25-10 provides an explanation of the command output.

Table 25-10 show ipv6 ospf neighbor routerid Output Details

Output Field	What It Displays...
Interface	Interface of the local router.
Area ID	OSPFv3 area ID associated with the interface.
Options	An integer value that indicates the optional OSPFv3 capabilities supported by the neighbor. These are listed in its Hello packets. This enables received Hello Packets to be rejected (that is, neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPFv3 capabilities.
Router Priority	Router priority for the specified interface.
Dead Timer Due	Amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.
State	State of the neighboring routers.
Events	Number of times this neighbor relationship has changed state, or an error has occurred.
Retransmission Queue Length	Integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

show ipv6 ospf range

This command displays information about the area ranges for the specified area.

Syntax

show ipv6 ospf range *areaid*

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Example

This example displays range information for area 20.

```
C3(su)->router#show ipv6 ospf range 20
    Area ID     IPv6 Prefix/Prefix Length    Lsdb Type    Advertisement
--------------- ------------------------- --------------- -------------
0.0.0.20        3345:1234::/64            Summary Link    Enabled
```

Table 25-11 provides an explanation of the command output.

Table 25-11 show ipv6 ospf range Output Details

Output Field	What It Displays...
Area ID	The area ID of the requested OSPFv3 area.
IPv6 Prefix/Prefix Length	An IPv6 prefix and length which represents a configured area range.
Lsdb Type	The type of link advertisement associated with this area range.
Advertisement	The status of the advertisement: enabled or disabled.

show ipv6 ospf stub table

This command displays the OSPFv3 stub table, if OSPFv3 is initialized on the switch.

Syntax

```
show ipv6 ospf stub table
```

Parameters

None.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Example

This example displays the OSPFv3 stub table information.

```
C3(su)->router# show ipv6 ospf stub table

AreaId           TypeofService Metric Val Import SummaryLSA
---------------- ------------- ---------- -----------------
0.0.0.20         Normal        1          Enable
```

Table 25-12 provides an explanation of the command output.

Table 25-12 show ipv6 ospf stub table Output Details

Output Field	What It Displays...
Area ID	A 32-bit identifier for the created stub area.
Type of Service	Type of service associated with the stub metric. For this release, Normal TOS is the only supported type.
Metric Val	The metric value is applied based on the TOS. It defaults to the least metric of the type of service among the interfaces to other areas. The OSPFv3 cost for a route is a function of the metric value.
Import Summary LSA	Controls the import of summary LSAs into stub areas.

show ipv6 ospf virtual-link

This command displays the OSPFv3 virtual interface information for a specific area and neighbor.

Syntax

show ipv6 ospf virtual-link *areaid neighborid*

Parameters

areaid	Specifies the area ID in IP address format (dotted-quad) or as a decimal value.
neighborid	Specifies the neighbor by its router ID, specified in 32-bit dotted quad format.

Defaults

None.

Mode

Router privileged execution: C3(su)->router#

Example

This information displays virtual link information for area ID 10 and the neighbor with router ID of 3.3.3.3.

```
C3(su)->router(Config)#show ipv6 ospf virtual-link 10 3.3.3.3
Area ID                                    10
Neighbor IP Address                        3.3.3.3
Hello Interval                             10
Dead Interval                              40
Iftransit Delay Interval                   1
Retransmit Interval                        5
State                                      DOWN
Metric                                     0
Neighbor State                             DOWN
```

Table 25-13 provides an explanation of the command output.

Table 25-13 show ipv6 ospf virtual-link Output Details

Output Field	What It Displays...
Area ID	The area id of the requested OSPFv3 area.
Neighbor Router ID	The input neighbor Router ID.
Hello Interval	The configured hello interval for the OSPFv3 virtual interface.
Dead Interval	The configured dead interval for the OSPFv3 virtual interface.
Iftransit Delay Interval	The configured transit delay for the OSPFv3 virtual interface.
Retransmit Interval	The configured retransmit interval for the OSPFv3 virtual interface.
State	The OSPFv3 Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPFv3 interface.

Table 25-13 show ipv6 ospf virtual-link Output Details (Continued)

Output Field	What It Displays...
Metric	The metric of this virtual link.
Neighbor State	The state of the neighbor. States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.

26

Authentication and Authorization Configuration

This chapter describes the following authentication and authorization commands and how to use them. For information about using the TACACS+ authentication method for management, see Chapter 27, **TACACS+ Configuration**.

Note: An Enterasys Networks Feature Guide document containing an in-depth discussion of authentication and authorization configuration is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

Overview of Authentication and Authorization Methods

The following methods are available for controlling which users are allowed to access, monitor, and manage the switch.

- Login user accounts and passwords – used to log in to the CLI via a Telnet connection or local COM port connection. For details, refer to "Setting User Accounts and Passwords" on page 3-2.
- Host Access Control Authentication (HACA) – authenticates user access of Telnet management, console local management and WebView via a central RADIUS Client/Server or

TACACS+ application. When RADIUS or TACACS+ is enabled, this essentially overrides login user accounts. When HACA is active per a valid RADIUS or TACACS+ configuration, the user names and passwords used to access the switch via Telnet, SSH, WebView, and COM ports will be validated against the configured RADIUS server. Only in the case of a RADIUS timeout will those credentials be compared against credentials locally configured on the switch. For details, refer to "Configuring RADIUS" on page 26-6.

- SNMP user or community names – allows access to the SecureStack C3 switch via a network SNMP management application. To access the switch, you must enter an SNMP user or community name string. The level of management access is dependent on the associated access policy. For details, refer to Chapter 8.
- 802.1X Port Based Network Access Control using EAPOL (Extensible Authentication Protocol) – provides a mechanism via a RADIUS server for administrators to securely authenticate and grant appropriate access to end user devices communicating with SecureStack C3 ports. For details on using CLI commands to configure 802.1X, refer to "Configuring 802.1X Authentication" on page 26-15.

Note: To configure EAP pass-through, which allows client authentication packets to be forwarded through the switch to an upstream device, 802.1X authentication must be globally disabled with the **set dot1x** command.

- MAC Authentication – provides a mechanism for administrators to securely authenticate source MAC addresses and grant appropriate access to end user devices communicating with SecureStack C3 ports. For details, refer to "Configuring MAC Authentication" on page 26-25.
- Multiple Authentication Methods – allows users to authenticate using multiple methods of authentication on the same port. For details, refer to "Configuring Multiple Authentication Methods" on page 26-37.
- Multi-User Authentication —allows multiple users and devices on the same port to authenticate using any supported authentication method. Each user or device can be mapped to the same or different roles using Enterasys policy for access control, VLAN authorization, traffic rate limiting, and quality of service. This is the most flexible and preferred method to use for VoIP (PC daisy chained to a phone). For details, refer to "About Multi-User Authentication" on page 26-37. Refer to Appendix A, **Policy and Authentication Capacities**, for a listing of the number of users per port supported by the SecureStack C3.
- User + IP Phone (Legacy feature) — The User + IP Phone authentication feature provides legacy support for authentication and authorization of two devices, specifically a PC cascaded with a VLAN-tagging IP phone, on a single port on the `switch`. The IP phone must authenticate using MAC or 802.1X authentication, but the user may authenticate by any method. This feature allows both the user's PC and IP phone to simultaneously authenticate on a single port and each receive a unique level of network access. For details, refer to "Configuring User + IP Phone Authentication" on page 26-48.

Note: User + IP Phone authentication is a legacy feature that should only be used if you have already implemented User + IP Phone in your network with switches that do not support true multi-user authentication.

- RFC 3580 tunnel attributes provide a mechanism to contain an 802.1X, MAC, or PWA authenticated user to a VLAN regardless of the PVID. This feature dynamically assigns a VLAN based on the RFC 3580 tunnel attributes returned in the RADIUS accept message. Refer to "Configuring VLAN Authorization (RFC 3580)" on page 26-49.
- Configuring Policy Maptable Response — allows you to define how the system should handle allowing an authenticated user onto a port based on the contents of the RADIUS server Access-Accept reply. There are three possible response settings: tunnel mode, policy mode, or

both tunnel and policy, also known as hybrid authentication mode. Refer to "Configuring Policy Maptable Response" on page 26-52.

- MAC Locking – locks a port to one or more MAC addresses, preventing the use of unauthorized devices and MAC spoofing on the port For details, refer to "Configuring MAC Locking" on page 26-57.
- Port Web Authentication (PWA) – passes all login information from the end station to a RADIUS server for authentication before allowing a user to access the network . PWA is an alternative to 802.1X and MAC authentication. For details, refer to "Configuring Port Web Authentication (PWA)" on page 26-68.
- Secure Shell (SSH) – provides secure Telnet. For details, refer to "Configuring Secure Shell (SSH)" on page 26-80.
- IP Access Lists (ACLs) – permits or denies access to routing interfaces based on protocol and inbound and/or outbound IP address restrictions configured in access lists. For details, refer to "Configuring Access Lists" on page 26-82.
- TACACS+ (Terminal Access Controller Access-Control System Plus) — a security protocol developed by Cisco Systems that can be used as an alternative to the standard RADIUS security protocol (RFC 2865). TACACS+ runs over TCP and encrypts the body of each packet. Refer to Chapter 27, **TACACS+ Configuration**, for information about the commands used to configure TACACS+.

RADIUS Filter-ID Attribute and Dynamic Policy Profile Assignment

If you configure an authentication method that requires communication with a RADIUS server, you can use the RADIUS Filter-ID attribute to dynamically assign a policy profile and/or management level to authenticating users and/or devices.

The RADIUS Filter-ID attribute is simply a string that is formatted in the RADIUS Access-Accept packet sent back from the RADIUS server to the switch during the authentication process.

Each user can be configured in the RADIUS server database with a RADIUS Filter-ID attribute that specifies the name of the policy profile and/or management level the user should be assigned upon successful authentication. During the authentication process, when the RADIUS server returns a RADIUS Access-Accept message that includes a Filter-ID matching a policy profile name configured on the switch, the switch then dynamically applies the policy profile to the physical port the user/device is authenticating on.

Filter-ID Attribute Formats

Enterasys Networkssupports two Filter-ID formats — "decorated" and "undecorated." The decorated format has three forms:

- To specify the policy profile to assign to the authenticating user (network access authentication):

  Enterasys:version=1:policy=*string*

  where *string* specifies the policy profile name. Policy profile names are case-sensitive.

- To specify a management level (management access authentication):

  Enterasys:version=1:mgmt=*level*

  where *level* indicates the management level, either **ro**, **rw**, or **su**.

- To specify both management level and policy profile:

  Enterasys:version=1:mgmt=*level*:policy=*string*

The undecorated format is simply a string that specifies a policy profile name. The undecorated format cannot be used for management access authentication.

Decorated Filter-IDs are processed first by the switch. If no decorated Filter-IDs are found, then undecorated Filter-IDs are processed. If multiple Filter-IDs are found that contain conflicting values, a Syslog message is generated.

Setting the Authentication Login Method

Purpose

To configure the authentication login method to be used for management.

Commands

The commands used to configure the authentication login method are listed below.

show authentication login

Use this command to display the current authentication login method for management.

Syntax

```
show authentication login
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example shows how to display the current authentication login method.

```
C3(rw)->show authentication login
Current authentication login is any
```

set authentication login

Use this command to set the authentication login method.

Syntax

```
set authentication login {any | local | radius | tacacs}
```

Parameters

any	Specifies that the authentication protocol will be selected using the following precedence order: • TACACS+ • RADIUS • Local
local	Specifies that the local network password settings will be used for authentication login.
radius	Specifies that RADIUS will be used for authentication login.
tacacs	Specifies that TACACS+ will be used for authentication login.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to set the authentication login method to use the local password settings:

```
C3(rw)->set authentication login local
```

clear authentication login

Use this command to reset the authentication login method to the default setting of “any”.

Syntax

```
clear authentication login
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to reset the authentication login method.

```
C3(rw)->clear authentication login
```

Configuring RADIUS

Purpose

To perform the following:

- Review the RADIUS client/server configuration on the switch.
- Enable or disable the RADIUS client.
- Set local and remote login options.
- Set primary and secondary server parameters, including IP address, timeout period, authentication realm, and number of user login attempts allowed.
- Reset RADIUS server settings to default values.
- Configure a RADIUS accounting server.
- Configure the interface used for the source IP address of the RADIUS application when generating RADIUS packets.

Commands

show radius

Use this command to display the current RADIUS client/server configuration.

Syntax

show radius [**status** | **retries** | **timeout** | **server** [*index* **| all**]]

Parameters

status	(Optional) Displays the RADIUS server's enable status.
retries	(Optional) Displays the number of retry attempts before the RADIUS server times out.
timeout	(Optional) Displays the maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin.

server	(Optional) Displays RADIUS server configuration information.
index | **all**	For use with the **server** parameter to show server configuration for all servers or a specific RADIUS server as defined by an index.

Defaults

If no parameters are specified, all RADIUS configuration information will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display RADIUS configuration information:

```
C3(rw)->show radius
 RADIUS status:    Enabled
 RADIUS retries:   3
 RADIUS timeout:   20 seconds
 RADIUS Server     IP Address      Auth-Port  Realm-Type
 --------------    ----------      ---------  -----------------
 10                172.16.20.10      1812     management-access
```

Table 26-1 provides an explanation of the command output.

Table 26-1 show radius Output Details

Output Field	What It Displays...
RADIUS status	Whether RADIUS is **enabled** or **disabled**.
RADIUS retries	Number of retry attempts before the RADIUS server times out. The default value of **3** can be reset using the **set radius** command as described in “set radius” on page 26-7.
RADIUS timeout	Maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin. The default value of **20** can be reset using the **set radius** command as described in “set radius” on page 26-7.
RADIUS Server	RADIUS server’s index number, IP address, and UDP authentication port.
Realm-Type	Realm defines who has to go through the RADIUS server for authentication. • Management-access: This means that anyone trying to access the switch (Telnet, SSH, Local Management) has to authenticate through the RADIUS server. • Network-access: This means that all the users have to authenticate to a RADIUS server before they are allowed access to the network. • Any-access: Means that both Management-access and Network-access have been enabled.

set radius

Use this command to enable, disable, or configure RADIUS authentication.

Syntax

set radius {**enable** | **disable**} | {**retries** *number-of-retries*} | {**timeout** *timeout*} | {**server** *index ip-address port* [*secret-value*] [**realm** {**management-access** | **any** | **network-access**}} | {**realm** {**management-access** | **any** | **network-access**} {*index*| **all**}}

Parameters

enable | **disable**	Enables or disables the RADIUS client.
retries *number-of-retries*	Specifies the number of retry attempts before the RADIUS server times out. Valid values are from **0** to **10**. Default is **3**.
timeout *timeout*	Specifies the maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin. Valid values are from **1** to **30**. Default is **20** seconds.
server *index ip_address port*	Specifies the index number, IP address and the UDP authentication port for the RADIUS server.
secret-value	(Optional) Specifies an encryption key to be used for authentication between the RADIUS client and server.
realm management-access | **any** | **network-access**	Realm allows you to define who has to go through the RADIUS server for authentication. • **management-access**: This means that anyone trying to access the switch (Telnet, SSH, Local Management) has to authenticate through the RADIUS server. • **network-access**: This means that all the users have to authenticate to a RADIUS server before they are allowed access to the network. • **any**: Means that both management-access and network-access have been enabled. **Note:** If the **management-access** or **any** access realm has been configured, the local "admin" account is disabled for access to the switch using the console, Telnet, or Local Management. Only the **network-access** realm allows access to the local "admin" account.
index | **all**	Applies the realm setting to a specific server or to all servers.

Defaults

If *secret-value* is not specified, none will be applied.

If **realm** is not specified, the **any** access realm will be used.

Mode

Switch command, read-write.

Usage

The SecureStack C3 device allows up to 10 RADIUS servers to be configured, with up to two servers active at any given time.

The RADIUS client can only be enabled on the switch once a RADIUS server is online, and its IP address(es) has been configured with the same password the RADIUS client will use.

Examples

This example shows how to enable the RADIUS client for authenticating with RADIUS server 1 at IP address 192.168.6.203, UDP authentication port 1812, and an authentication password of "pwsecret." As previously noted, the "server secret" password entered here must match that already configured as the Read-Write (rw) password on the RADIUS server:

```
C3(su)->set radius server 1 192.168.6.203 1812 pwsecret
```

This example shows how to set the RADIUS timeout to 5 seconds:

```
C3(su)->set radius timeout 5
```

This example shows how to set RADIUS retries to 10:

```
C3(su)->set radius retries 10
```

This example shows how to force any management-access to the switch (Telnet, web, SSH) to authenticate through a RADIUS server. The **all** parameter at the end of the command means that any of the defined RADIUS servers can be used for this Authentication.

```
C3(rw)->set radius realm management-access all
```

clear radius

Use this command to clear RADIUS server settings.

Syntax

clear radius [**retries**] | [**timeout**] | [**server** {*index* | **all** | **realm** {*index* | **all**}}]

Parameters

retries	Resets the maximum number of attempts a user can contact the RADIUS server before timing out to **3**.
timeout	Resets the maximum amount of time to establish contact with the RADIUS server before timing out to **20** seconds.
server	Deletes server settings.
index | **all**	For use with the **server** parameter to clear the server configuration for all servers or a specific RADIUS server as defined by an index.
realm	Resets the realm setting for all servers or a specific RADIUS server as defined by an index.

Mode

Switch command, read-write.

Defaults

None.

Examples

This example shows how to clear all settings on all RADIUS servers:

```
C3(su)->clear radius server all
```

This example shows how to reset the RADIUS timeout to the default value of 20 seconds:

```
C3(su)->clear radius timeout
```

show radius accounting

Use this command to display the RADIUS accounting configuration. This transmits accounting information between a network access server and a shared accounting server.

Syntax

show radius accounting [**server**] | [**counter** *ip-address*] | [**retries**] | [**timeout**]

Parameters

server	(Optional) Displays one or all RADIUS accounting server configurations.
counter *ip-address*	(Optional) Displays counters for a RADIUS accounting server.
retries	(Optional) Displays the maximum number of attempts to contact the RADIUS accounting server before timing out.
timeout	(Optional) Displays the maximum amount of time before timing out.

Mode

Switch command, read-only.

Defaults

If no parameters are specified, all RADIUS accounting configuration information will be displayed.

Example

This example shows how to display RADIUS accounting configuration information. In this case, RADIUS accounting is not currently enabled and global default settings have not been changed. One server has been configured.

For details on enabling and configuring RADIUS accounting, refer to "set radius accounting" on page 26-10:

```
C3(ro)->show radius accounting

RADIUS accounting status:      Disabled
 RADIUS Acct Server  IP Address  Acct-Port Retries Timeout Status
 ------------------  ----------  --------- ------- ------- ------
 1                   172.16.2.10  1856      3       20      Disabled
```

set radius accounting

Use this command to configure RADIUS accounting.

Syntax

set radius accounting {[**enable** | **disable**] [**retries** *retries*] [**timeout** *timeout*] [**server** *ip_address port* [*server-secret*]

Parameters

enable | **disable**	Enables or disables the RADIUS accounting client.
retries *retries*	Sets the maximum number of attempts to contact a specified RADIUS accounting server before timing out. Valid retry values are **0** - **10**.

timeout *timeout*	Sets the maximum amount of time (in seconds) to establish contact with a specified RADIUS accounting server before timing out. Valid timeout values are **1** - **30**.
server *ip_address port server-secret*	Specifies the accounting server's: • IP address • UDP authentication port (**0** - **65535)** • *server-secret* (Read-Write password to access this accounting server. Device will prompt for this entry upon creating a server instance, as shown in the example below.)

Mode

Switch command, read-write.

Defaults

None.

Examples

This example shows how to enable the RADIUS accounting client for authenticating with the accounting server at IP address 10.2.4.12, UDP authentication port 1800. As previously noted, the "server secret" password entered here must match that already configured as the Read-Write (rw) password on the RADIUS accounting server:

```
C3(su)->set radius accounting server 10.2.4.12 1800
Enter secret:
Re-enter secret:
```

This example shows how to set the RADIUS accounting timeout to 30 seconds:

```
C3(su)->set radius accounting timeout 30
```

This example shows how to set RADIUS accounting retries to 10:

```
C3(su)->set radius accounting retries 10
```

clear radius accounting

Use this command to clear RADIUS accounting configuration settings.

Syntax

clear radius accounting {**server** *ip-address* | **retries** | **timeout** | **counter**}

Parameters

server *ip-address*	Clears the configuration on one or more accounting servers.
retries	Resets the retries to the default value of 3.
timeout	Resets the timeout to 5 seconds.
counter	Clears counters.

Mode

Switch command, read-write.

Defaults

None.

Example

This example shows how to reset the RADIUS accounting timeout to 5 seconds.

```
C3(su)->clear radius accounting timeout
```

show radius interface

Use this command to display the interface used for the source IP address of the RADIUS application when generating RADIUS packets.

Syntax

show radius interface

Parameters

None.

Defaults

None.

Mode

Switch mode, read-only.

Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the RADIUS application.

```
C3(rw)->show radius interface
loopback 1  192.168.10.1
```

set radius interface

Use this command to specify the interface used for the source IP address of the RADIUS application when generating RADIUS packets.

Syntax

set radius interface {**loopback** *loop-ID* | **vlan** *vlan-ID*}

Parameters

loopback *loop-ID*	Specifies the loopback interface to be used. The value of *loop-ID* can range from 0 to 7.
vlan *vlan-ID*	Specifies the VLAN interface to be used. The value of vlan-ID can range from 1 to 4093.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command allows you to configure the source IP address used for the source IP address of the RADIUS application when generating RADIUS packets. Any of the management interfaces, including VLAN routing interfaces, can be configured as the source IP address used in packets generated by the RADIUS application.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the IP address of the Host interface, if configured, will be used for both the source IP address and NAS-IP. If no interface is specified and no Host address is configured, the source IP address will be the address of the routed interface on which the packet egresses. If loopback 0 has been configured, the NAS-IP will be set to the IP address of loopback 0. Otherwise, the NAS-IP will be zero.

Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the RADIUS application source IP address.

```
C3(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
C3(rw)->router(Config-if(Vlan 100))#exit
C3(rw)->router(Config)#exit
C3(rw)->router#exit
C3(rw)->router>exit
C3(rw)->set radius interface vlan 100

C3(rw)->show radius interface
vlan 100  192.168.10.1
```

clear radius interface

Use this command to clear the interface used for the source IP address of the RADIUS application back to the default of the Host interface, if configured. If no Host address is configured, the source IP address will be the address of the routed interface on which the packet egresses.

Syntax

```
clear radius interface
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This command returns the interface used for the source IP address of the RADIUS application back to the default of the Host interface.

```
C3(rw)->show radius interface
vlan 100  192.168.10.1
C3(rw)->clear radius interface
C3(rw)->
```

Configuring 802.1X Authentication

Purpose

To review and configure 802.1X authentication for one or more ports using EAPOL (Extensible Authentication Protocol). 802.1X controls network access by enforcing user authorization on selected ports, which results in allowing or denying network access according to RADIUS server configuration.

Note: To configure EAP pass-through, which allows client authentication packets to be forwarded through the switch to an upstream device, 802.1X authentication must be globally disabled with the **set dot1x** command ("set dot1x" on page 26-18).

Commands

show dot1x

Use this command to display 802.1X status, diagnostics, statistics, and reauthentication or initialization control information for one or more ports.

Syntax

`show dot1x` [**`auth-diag`**] [**`auth-stats`**] [**`port`** [**`init`** | **`reauth`**]] [*`port-string`*]

Parameters

auth-diag	(Optional) Displays authentication diagnostics information.
auth-stats	(Optional) Displays authentication statistics.
port init | **reauth**	(Optional) Displays the status of port initialization and reauthentication control for the port.
port-string	(Optional) Displays information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If no parameters are specified, 802.1X status will be displayed.

If *port-string* is not specified, information for all ports will be displayed.

Mode

Switch command, read-only.

Examples

This example shows how to display 802.1X status:

```
C3(su)->show dot1x
DOT1X is disabled.
```

This example shows how to display authentication diagnostics information for ge.1.1:

```
C3(su)->show dot1x auth-diag ge.1.1

Port : 1   Auth-Diag
Enter Connecting:                       0
EAP Logoffs While Connecting:           0
Enter Authenticating:                   0
Success While Authenticating            0
Timeouts While Authenticating:          0
Fails While Authenticating:             0
ReAuths While Authenticating:           0
EAP Starts While Authenticating:        0
EAP logoff While Authenticating:        0
Backend Responses:                      0
Backend Access Challenges:              0
Backend Others Requests To Supp:        0
Backend NonNak Responses From:          0
Backend Auth Successes:                 0
Backend Auth Fails:                     0
```

This example shows how to display authentication statistics for ge.1.1:

```
C3(su)->show dot1x auth-stats ge.1.1
Port: 1   Auth-Stats
EAPOL Frames Rx:              0
EAPOL Frames Tx:              0
EAPOL Start Frames Rx:        0
EAPOL Logoff Frames Rx:       0
EAPOL RespId Frames Rx:       0
EAPOL Resp Frames Rx:         0
EAPOL Req Frames Tx:          0
EAP Length Error Frames Rx:   0
Last EAPOL Frame Version:     0
Last EAPOL Frame Source:      00:00:00:00:00:00
```

This example shows how to display the status of port reauthentication control for ge.1.1 through ge.1.6:

```
C3(su)->show dot1x port reauth ge.1.1-6
 Port 1: Port reauthenticate:     FALSE
 Port 2: Port reauthenticate:     FALSE
 Port 3: Port reauthenticate:     FALSE
 Port 4: Port reauthenticate:     FALSE
 Port 5: Port reauthenticate:     FALSE
 Port 6: Port reauthenticate:     FALSE
```

show dot1x auth-config

Use this command to display 802.1X authentication configuration settings for one or more ports.

Syntax

```
show dot1x auth-config [authcontrolled-portcontrol] [maxreq] [quietperiod]
[reauthenabled] [reauthperiod] [servertimeout] [supptimeout] [txperiod]
[port-string]
```

Parameters

authcontrolled-portcontrol	(Optional) Displays the current value of the controlled Port control parameter for the port.
maxreq	(Optional) Displays the value set for maximum requests currently in use by the backend authentication state machine.
quietperiod	(Optional) Displays the value set for quiet period currently in use by the authenticator PAE state machine.
reauthenabled	(Optional) Displays the state of reauthentication control used by the Reauthentication Timer state machine.
reauthperiod	(Optional) Displays the value, in seconds, set for the reauthentication period used by the reauthentication timer state machine.
servertimeout	(Optional) Displays the server timeout value, in seconds, currently in use by the backend authentication state machine.
supptimeout	(Optional) Displays the authentication supplicant timeout value, in seconds, currently in use by the backend authentication state machine.
txperiod	(Optional) Displays the transmission period value, in seconds, currently in use by the authenticator PAE state machine.
port-string	(Optional) Limits the display of desired information information to specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If no parameters are specified, all 802.1X settings will be displayed.

If *port-string* is not specified, information for all ports will be displayed.

Mode

Switch command, read-only.

Examples

This example shows how to display the EAPOL port control mode for ge.1.1:

```
C3(su)->show dot1x auth-config authcontrolled-portcontrol ge.1.1
Port 1: Auth controlled port control:             Auto
```

This example shows how to display the 802.1X quiet period settings for ge.1.1:

```
C3(su)->show dot1x auth-config quietperiod ge.1.1
 Port 1: Quiet period:         30
```

This example shows how to display all 802.1X authentication configuration settings for ge.1.1:

```
C3(ro)->show dot1x auth-config ge.1.1
```

```
Port : 1    Auth-Config
 PAE state:                              Initialize
 Backend auth state:                     Initialize
 Admin controlled directions:            Both
 Oper controlled directions:             Both
 Auth controlled port status:            Authorized
 Auth controlled port control:           Auto
 Quiet period:                  60
 Transmission period:           30
 Supplicant timeout:            30
 Server timeout:                30
 Maximum requests:              2
 Reauthentication period:       3600
 Reauthentication control:      Disabled
```

set dot1x

Use this command to enable or disable 802.1X authentication, to reauthenticate one or more access entities, or to reinitialize one or more supplicants.

Syntax

set dot1x {**enable** | **disable** | **port** {**init** | **reauth**} {**true** | **false**} [*port-string*]*}*

Parameters

enable | **disable**	Enables or disables 802.1X.
port	Enable or disable 802.1X reauthentication or initialization control on one or more ports.
init | **reauth**	Configure initialization or reauthentication control.
true | **false**	Enable (true) or disable (false) reinitialization/reauthentication.
port-string	(Optional) Specifies the port(s) to reinitialize or reauthenticate.

Defaults

If no ports are specified, the reinitialization or reauthentication setting will be applied to all ports.

Mode

Switch command, read-write.

Usage

Disabling 802.1X authentication globally, by not entering a specific *port-string* value, will enable the EAP pass-through feature. EAP pass-through allows client authentication packets to be forwarded unmodified through the switch to an upstream device.

Examples

This example shows how to enable 802.1X:

```
C3(su)->set dot1x enable
```

This example shows how to reinitialize ge.1.2:

```
C3(rw)->set dot1x port init true ge.1.2
```

set dot1x auth-config

Use this command to configure 802.1X authentication.

Syntax

```
set dot1x auth-config {[authcontrolled-portcontrol {auto | forced-auth |
forced-unauth}] [maxreq value] [quietperiod value] [reauthenabled {false | true}]
[reauthperiod value] [servertimeout timeout] [supptimeout timeout] [txperiod
value]} [port-string]
```

Parameters

authcontrolled-portcontrol auto | **forced-auth** | **forced-unauth**	Specifies the 802.1X port control mode. • **auto** – Set port control mode to auto controlled port control. This is the default value. • **forced-auth –** Set port control mode to ForcedAuthorized controlled port control. • **forced-unauth –** Set port control mode to ForcedUnauthorized controlled port control.
maxreq *value*	Specifies the maximum number of authentication requests allowed by the backend authentication state machine. Valid values are **1 – 10**. Default value is 2.
quietperiod *value*	Specifies the time (in seconds) following a failed authentication before another attempt can be made by the authenticator PAE state machine. Valid values are **0 – 65535**. Default value is 60 seconds.
reauthenabled false | **true**	Enables (**true**) or disables (**false**) reauthentication control of the reauthentication timer state machine. Default value is false.
reauthperiod *value*	Specifies the time lapse (in seconds) between attempts by the reauthentication timer state machine to reauthenticate a port. Valid values are **0 – 65535**. Default value is 3600 seconds.
servertimeout *timeout*	Specifies a timeout period (in seconds) for the authentication server, used by the backend authentication state machine. Valid values are **1 – 300**. Default value is 30 seconds.
supptimeout *timeout*	Specifies a timeout period (in seconds) for the authentication supplicant used by the backend authentication state machine. Valid values are **1 – 300**. Default value is 30 seconds.
txperiod *value*	Specifies the period (in seconds) which passes between authenticator PAE state machine EAP transmissions. Valid values are **0 – 65535**. Default value is 30 seconds.
port-string	(Optional) Limits the configuration of desired settings to specified port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, authentication parameters will be set on all ports.

Mode

Switch command, read-write.

Examples

This example shows how to enable reauthentication control on ports ge.1.1-3:

```
C3(su)->set dot1x auth-config reauthenabled true ge.1.1-3
```

This example shows how to set the 802.1X quiet period to 120 seconds on ports ge.1.1-3:

```
C3(su)->set dot1x auth-config quietperiod 120 ge.1.1-3
```

clear dot1x auth-config

Use this command to reset 802.1X authentication parameters to default values on one or more ports.

Syntax

clear dot1x auth-config [**authcontrolled-portcontrol**] [**maxreq**] [**quietperiod**] [**reauthenabled**] [**reauthperiod**] [**servertimeout**] [**supptimeout**] [**txperiod**] [*port-string*]

Parameters

authcontrolled-portcontrol	(Optional) Resets the 802.1X port control mode to **auto**.
maxreq	(Optional) Resets the maximum requests value to **2**.
quietperiod	(Optional) Resets the quiet period value to **60** seconds.
reauthenabled	(Optional) Resets the reauthentication control state to disabled (**false**).
reauthperiod	(Optional) Resets the reauthentication period value to **3600** seconds.
servertimeout	(Optional) Resets the server timeout value to **30** seconds.
supptimeout	(Optional) Resets the authentication supplicant timeout value to **30** seconds.
txperiod	(Optional) Resets the transmission period value to **30** seconds.
port-string	(Optional) Resets settings on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If no parameters are specified, all authentication parameters will be reset.

If *port-string* is not specified, parameters will be set on all ports.

Mode

Switch command, read-write.

Examples

This example shows how to reset the 802.1X port control mode to auto on all ports:

```
C3(su)->clear dot1x auth-config authcontrolled-portcontrol
```

This example shows how to reset reauthentication control to disabled on ports ge.1.1-3:

```
C3(su)->clear dot1x auth-config reauthenabled ge.1.1-3
```

This example shows how to reset the 802.1X quiet period to 60 seconds on ports ge.1.1-3:

```
C3(su)->clear dot1x auth-config quietperiod ge.1.1-3
```

show eapol

Use this command to display EAPOL status or settings for one or more ports.

Syntax

show eapol [*port-string*]

Parameters

port-string	(Optional) Displays EAPOL status for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, only EAPOL enable status will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display EAPOL status for ports ge.1.1-3:

```
C3(su)->show eapol ge.1.1-3
EAPOL is disabled.

Port      Authentication State    Authentication Mode
--------   --------------------   --------------------
ge.1.1     Initialize             Auto
ge.1.2     Initialize             Auto
ge.1.3     Initialize             Auto
```

Table 26-2 provides an explanation of the command output. For details on using the **set eapol** command to enable the protocol and assign an authentication mode, refer to "set eapol" on page 26-23.

Table 26-2 show eapol Output Details

Output Field	What It Displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
Authentication State	Current EAPOL authentication state for each port. Possible internal states for the authenticator (switch) are: • **initialize**: A port is in the initialize state when: – authentication is disabled, – authentication is enabled and the port is not linked, or – authentication is enabled and the port is linked. (In this case very little time is spent in this state, it immediately transitions to the connecting state, via disconnected. • **disconnected**: The port passes through this state on its way to connected whenever the port is reinitialized, via link state change, reauthentication failure, or management intervention. • **connecting**: While in this state, the authenticator sends request/ID messages to the end user. • **authenticating**: The port enters this state from connecting after receiving a response/ID from the end user. It remains in this state until the entire authentication exchange between the end user and the authentication server completes. • **authenticated**: The port enters this state from authenticating state after the exchange completes with a favorable result. It remains in this state until linkdown, logoff, or until a reauthentication begins. • **aborting**: The port enters this state from authenticating when any event occurs that interrupts the login exchange. • **held**: After any login failure the port remains in this state for the number of seconds equal to quietPeriod (can be set using MIB). • **forceAuth**: Management is allowing normal, unsecured switching on this port. • **forceUnauth**: Management is preventing any frames from being forwarded to or from this port.
Authentication Mode	Mode enabling network access for each port. Modes include: • **Auto**: Frames are forwarded according to the authentication state of each port. • **Forced Authorized Mode**: Meant to disable authentication on a port. It is intended for ports that support ISLs and devices that cannot authenticate, such as printers and file servers. If a default policy is applied to the port via the policy profile MIB, then frames are forwarded according to the configuration set by that policy, otherwise frames are forwarded according to the current configuration for that port. Authentication using 802.1X is not possible on a port in this mode. • **Forced Unauthorized Mode**: All frames received on the port are discarded by a filter. Authentication using 802.1X is not possible on a port in this mode.

set eapol

Use this command to enable or disable EAPOL port-based user authentication with the RADIUS server and to set the authentication mode for one or more ports.

Syntax

set eapol [**enable** | **disable**] [**auth-mode** {**auto** | **forced-auth** | **forced-unauth**} *port-string*

Parameters

enable | **disable**	Enables or disables EAPOL.
auth-mode	Specifies the authentication mode as:
auto | **forced-auth** | **forced-unauth**	• **auto** - Auto authorization mode. This is the default mode and will forward frames according to the authentication state of the port. For details on this mode, refer to Table 26-2. • **forced-auth** - Forced authorized mode, which disables authentication on the port. • **forced-unauth** - Forced unauthorized mode, which filters and discards all frames received on the port.
port-string	Specifies the port(s) on which to set EAPOL parameters. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Examples

This example shows how to enable EAPOL:

```
C3(su)->set eapol enable
```

This example shows how to enable EAPOL with forced authorized mode on port ge.1.1:

```
C3(su)->set eapol auth-mode forced-auth ge.1.1
```

clear eapol

Use this command to globally clear the EAPOL authentication mode, or to clear settings for one or more ports.

Syntax

clear eapol [**auth-mode**] [*port-string*]

Parameters

auth-mode	(Optional) Globally clears the EAPOL authentication mode.
port-string	Specifies the port(s) on which to clear EAPOL parameters. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If **auth-mode** is not specified, all EAPOL settings will be cleared.

If *port-string* is not specified, settings will be cleared for all ports.

Mode

Switch command, read-write.

Example

This example shows how to clear the EAPOL authentication mode for port ge.1.3:

```
C3(su)->clear eapol auth-mode ge.1.3
```

Configuring MAC Authentication

Purpose

To review, disable, enable and configure MAC authentication. This authentication method allows the device to authenticate source MAC addresses in an exchange with an authentication server. The authenticator (switch) selects a source MAC seen on a MAC-authentication enabled port and submits it to a backend client for authentication. The backend client uses the MAC address stored password, if required, as credentials for an authentication attempt. If accepted, a string representing an access policy and/or VLAN authorization may be returned. If present, the switch applies the associated policy rules and VLAN segmentation.

You can specify a mask to apply to MAC addresses when authenticating users through a RADIUS server (see "set macauthentication significant-bits" on page 26-35). The most common use of significant bit masks is for authentication of all MAC addresses for a specific vendor.

Commands

show macauthentication

Use this command to display MAC authentication information for one or more ports.

Syntax

show macauthentication [*port-string*]

Parameters

port-string	(Optional) Displays MAC authentication information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, MAC authentication information will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display MAC authentication information for ge.2.1 through 8:

```
C3(su)->show macauthentication ge.2.1-8
MAC authentication:           - enabled
MAC user password:            - NOPASSWORD
Port username significant bits  - 48

 Port     Port     Reauth     Auth     Auth      Reauthentications
          State    Period     Allowed  Allocated
 -------  -------- ---------- -------- --------- -----------------
 ge.2.1   disabled 3600       1        1         disabled
 ge.2.2   disabled 3600       1        1         disabled
 ge.2.3   disabled 3600       1        1         disabled
 ge.2.4   disabled 3600       1        1         disabled
 ge.2.5   disabled 3600       1        1         disabled
 ge.2.6   disabled 3600       1        1         disabled
 ge.2.7   disabled 3600       1        1         disabled
 ge.2.8   disabled 3600       1        1         disabled
```

Table 26-3 provides an explanation of the command output.

Table 26-3 show macauthentication Output Details

Output Field	What It Displays...
MAC authentication	Whether MAC authentication is globally enabled or disabled. Set using the **set macauthentication** command as described in "set macauthentication" on page 26-28.
MAC user password	User password associated with MAC authentication on the device. Set using the **set macauthentication password** command as described in "set macauthentication password" on page 26-28.
Port username significant bits	Number of significant bits in the MAC addresses to be used starting with the left-most bit of the vendor portion of the MAC address. The significant portion of the MAC address is sent as a user-name credential when the primary attempt to authenticate the full MAC address fails. Any other failure to authenticate the full address, (i.e., authentication server timeout) causes the next attempt to start once again with a full MAC authentication. Default value of 48 can be changed with the **set macauthentication significant-bits** command.
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
Port State	Whether or not MAC authentication is enabled or disabled on this port.

Table 26-3 show macauthentication Output Details (Continued)

Output Field	What It Displays...
Reauth Period	Reauthentication period for this port. Default value of **30** can be changed using the **set macauthentication reauthperiod** command (page 26-33).
Auth Allowed	Number of concurrent authentications supported on this port.
Auth Allocated	Maximum number of MAC authentications permitted on this port.
Reauthentications	Whether or not reauthentication is enabled or disabled on this port. Set using the **set macauthentication reauthentication** command (page 26-32).

show macauthentication session

Use this command to display the active MAC authenticated sessions.

Syntax

```
show macauthentication session
```

Parameters

None.

Defaults

If *port-string* is not specified, MAC session information will be displayed for all MAC authentication ports.

Mode

Switch command, read-only.

Usage

Changing the Reauth Period with the set macauthentication reauthperiod command does not affect current sessions. New sessions display the correct period.

Example

This example shows how to display MAC session information:

```
C3(su)->show macauthentication session
Port       MAC Address      Duration   Reauth Period   Reauthentications
-----    -----------------  ---------- -------------   -----------------
ge.1.2   00:60:97:b5:4c:07  0,00:52:31  3600           disabled
```

Table 26-4 provides an explanation of the command output.

Table 26-4 show macauthentication session Output Details

Output Field	What It Displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
MAC Address	MAC address associated with the session.
Duration	Time this session has been active.

Table 26-4 show macauthentication session Output Details (Continued)

Output Field	What It Displays...
Reauth Period	Reauthentication period for this port, set using the **set macauthentication reauthperiod** command described in "set macauthentication reauthperiod" on page 26-33.
Reauthentications	Whether or not reauthentication is enabled or disabled on this port. Set using the **set macauthentication reauthentication** command described in "set macauthentication reauthentication" on page 26-32.

set macauthentication

Use this command to globally enable or disable MAC authentication.

Syntax

set macauthentication {**enable** | **disable**}

Parameters

enable | **disable**	Globally enables or disables MAC authentication.

Mode

Switch command, read-write.

Defaults

None.

Example

This example shows how to globally enable MAC authentication:

```
C3(su)->set macauthentication enable
```

set macauthentication password

Use this command to set a MAC authentication password.

Syntax

set macauthentication password *password*

Parameters

password	Specifies a text string MAC authentication password.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the MAC authentication password to “macauth”:

```
C3(su)->set macauthentication password macauth
```

clear macauthentication password

Use this command to clear the MAC authentication password.

Syntax

clear macauthentication password

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the MAC authentication password:

```
C3(su)->clear macauthentication password
```

set macauthentication port

Use this command to enable or disable one or more ports for MAC authentication.

Syntax

set macauthentication port {**enable** | **disable**} *port-string*

Parameters

enable | **disable**	Enables or disables MAC authentication.
port-string	Specifies port(s) on which to enable or disable MAC authentication. For a detailed description of possible *port-string* values, refer to “Port String Syntax Used in the CLI” on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Usage

Enabling port(s) for MAC authentication requires globally enabling MAC authentication on the switch as described in "set macauthentication" on page 26-28, and then enabling it on a port-by-port basis. By default, MAC authentication is globally disabled and disabled on all ports.

Example

This example shows how to enable MAC authentication on ge.2.1 though 5:

```
C3(su)->set macauthentication port enable ge.2.1-5
```

set macauthentication portinitialize

Use this command to force one or more MAC authentication ports to re-initialize and remove any currently active sessions on those ports.

Syntax

set macauthentication portinitialize *port-string*

Parameters

port-string	Specifies the MAC authentication port(s) to re-initialize. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to force ge.2.1 through 5 to initialize:

```
C3(su)->set macauthentication portinitialize ge.2.1-5
```

set macauthentication portquietperiod

This sets the number of seconds following a failed authentication before another attempt may be made on the port.

Syntax

set macauthentication portquietperiod *time port-string*

Parameters

time	Period in seconds to wait after a failed authentication. By default, this is 30 seconds.
port-string	Specifies the ports for which the quit period is to be applied. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example sets port 1 to wait 5 seconds after a failed authentication attempt before a new attempt can be made:

```
C3(su)->set macauthentication portquietperiod 5 ge.1.1
```

clear macauthentication portquietperiod

This sets the quiet period back to the default value of 30 seconds.

Syntax

clear macauthentication portquietperiod [*port-string*]

Parameters

port-string	(Optional) Specifies the ports for which the quiet period is to be reset. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If a *port-string* is not specified then all ports will be set to the default port quiet period.

Mode

Switch command, read-write.

Example

This example resets the default quiet period on port 1:

```
C3(su)->clear macauthentication portquietperiod ge.1.1
```

set macauthentication macinitialize

Use this command to force a current MAC authentication session to re-initialize and remove the session.

Syntax

set macauthentication macinitialize *mac-addr*

Parameters

mac-addr	Specifies the MAC address of the session to re-initialize.

Mode

Switch command, read-write.

Defaults

None.

Example

This example shows how to force the MAC authentication session for address 00-60-97-b5-4c-07 to re-initialize:

```
C3(su)->set macauthentication macinitialize 00-60-97-b5-4c-07
```

set macauthentication reauthentication

Use this command to enable or disable reauthentication of all currently authenticated MAC addresses on one or more ports.

Syntax

`set macauthentication reauthentication {enable | disable}` *`port-string`*

Parameters

enable | **disable**	Enables or disables MAC reauthentication.
port-string	Specifies port(s) on which to enable or disable MAC reauthentication. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to enable MAC reauthentication on ge.4.1 though 5:

```
C3(su)->set macauthentication reauthentication enable ge.4.1-5
```

set macauthentication portreauthenticate

Use this command to force an immediate reauthentication of the currently active sessions on one or more MAC authentication ports.

Syntax

`set macauthentication portreauthenticate` *`port-string`*

Parameters

port-string	Specifies MAC authentication port(s) to be reauthenticated. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to force ge.2.1 though 5 to reauthenticate:

```
C3(su)->set macauthentication portreauthentication ge.2.1-5
```

set macauthentication macreauthenticate

Use this command to force an immediate reauthentication of a MAC address.

Syntax

`set macauthentication macreauthenticate` *`mac-addr`*

Parameters

mac-addr	Specifies the MAC address of the session to reauthenticate.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to force the MAC authentication session for address 00-60-97-b5-4c-07 to reauthenticate:

```
C3(su)->set macauthentication macreauthenticate 00-60-97-b5-4c-07
```

set macauthentication reauthperiod

Use this command to set the MAC reauthentication period (in seconds). This is the time lapse between attempts to reauthenticate any current MAC address authenticated to a port.

Syntax

`set macauthentication reauthperiod` *`time port-string`*

Parameters

time	Specifies the number of seconds between reauthentication attempts. Valid values are **1** - **4294967295**.
port-string	Specifies the port(s) on which to set the MAC reauthentication period. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Usage

Changing the Reauth Period with the **set macauthentication reauthperiod** command does not affect current sessions. New sessions will use the correct period.

Example

This example shows how to set the MAC reauthentication period to 7200 seconds (2 hours) on ge.2.1 through 5:

```
C3(su)->set macauthentication reauthperiod 7200 ge.2.1-5
```

clear macauthentication reauthperiod

Use this command to clear the MAC reauthentication period on one or more ports.

Syntax

clear macauthentication reauthperiod [*port-string*]

Parameters

port-string	(Optional) Clears the MAC reauthentication period on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, the reauthentication period will be cleared on all ports.

Mode

Switch command, read-write.

Example

This example shows how to globally clear the MAC reauthentication period:

```
C3(su)->clear macauthentication reauthperiod
```

set macauthentication significant-bits

Use this command to set the number of significant bits of the MAC address to use for authentication.

Syntax

`set macauthentication significant-bits` *`number`*

Parameters

number	Specifies the number of significant bits to be used for authentication.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command allows you to specify a mask to apply to MAC addresses when authenticating users through a RADIUS server. The most common use of significant bit masks is for authentication of all MAC addresses for a specific vendor.

On switches using MAC authentication, the MAC address of a user attempting to log in is sent to the RADIUS server as the user name. If access is denied, and if a significant bit mask has been configured (other than 48) with this command, the switch will apply the mask and resend the masked address to the RADIUS server. For example, if a user with MAC address of 00-16-CF-12-34-56 is denied access, and a 32 bit mask has been configured, the switch will apply the mask and resend a MAC address of 00-16-CF-12-00-00 to the RADIUS server.

To use a significant bits mask for authentication of devices by a particular vendor, specify a 24-bit mask, to mask out everything except the vendor portion of the MAC address.

Example

This example sets the MAC authentication significant bits mask to 24.

```
C3(su)->set macauthentication significant-bits 24
```

clear macauthentication significant-bits

Use this command to reset the number of significant bits of the MAC address to use for authentication to the default of 48.

Syntax

`clear macauthentication significant-bits`

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example resets the MAC authentication significant bits to 48.

```
C3(su)->clear macauthentication significant-bits
```

Configuring Multiple Authentication Methods

About Multiple Authentication Types

When enabled, multiple authentication types allows a user to authenticate using more than one method on the same port. In order for multiple authentication to function on the device, each possible method of authentication (MAC authentication, 802.1X, PWA) must be enabled globally and configured appropriately on the desired ports with its corresponding command set described in this chapter. The precedence configured for the authentication methods determines which authentication method is actually applied to the user, device, or port.

Multiple authentication mode must be globally enabled on the device using the set multiauth mode command. Authentication precedence can be configured with the set multiauth precedence command.

About Multi-User Authentication

Multi-user authentication refers to the ability to authenticate more than one user or device on the same port, with each user or device being provided the appropriate level of network resources based on policy.

When a single supplicant connected to an access layer port authenticates, a policy profile can be dynamically applied to all traffic on the port. When multi-user authentication is **not** implemented, and more than one supplicant is connected to a port, the firmware does not provision network resources on a per-user or per-device basis, even though different users or devices may require a different set of network resources.

In order to support provisioning network resources on a per-user basis, by applying the policy configured in the RADIUS filter-ID or RFC 3580 tunnel attributes for a given user or device, the switch must be the point of authentication for the attached devices. The RADIUS filter-ID and tunnel attributes are part of the RADIUS user account and are included in the RADIUS access-accept message response received by the switch from the authentication server.

The maximum number of multiple users supported per port depends on your platform. Refer to Appendix A, **Policy and Authentication Capacities** for a description of the multi-user capacities for this device. By default, the number of allowed users per port is set to 1. To configure the number of allowed users per port, use the **set multiauth port numusers** command. Use the **show multiauth port** command to display the current values of “Max users” and “Allowed users” per port.

Commands

show multiauth

Use this command to display multiple authentication system configuration.

Syntax

show multiauth

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display multiple authentication system configuration:

```
C3(rw)->show multiauth

Multiple authentication system configuration
------------------------------------------------
Supported types               : dot1x, pwa, mac
Maximum number of users       : 768
Current number of users       : 2
System mode                   : multi
Default precedence            : dot1x, pwa, mac
Admin precedence              : dot1x, pwa, mac
Operational precedence        : dot1x, pwa, mac
```

set multiauth mode

Use this command to set the system authentication mode to allow multiple authenticators simultaneously (802.1x, PWA, and MAC Authentication) on a single port, or to strictly adhere to 802.1x authentication.

Syntax

```
set multiauth mode {multi | strict}
```

Parameters

multi	Allows the system to use multiple authenticators simultaneously (802.1x, PWA, and MAC Authentication) on a port. This is the default mode.
strict	User must authenticate using 802.1x authentication before normal traffic (anything other than authentication traffic) can be forwarded.

Defaults

None.

Mode

Switch command, read-write.

Usage

Multiauth **multi** mode requires that MAC, PWA, and 802.1X authentication be enabled globally, and configured appropriately on the desired ports according to their corresponding command sets described in this chapter. Refer to "Configuring 802.1X Authentication" on page 26-15 and "Configuring MAC Authentication" on page 26-25 and "Configuring Port Web Authentication (PWA)" on page 26-68.

Example

This example shows how to enable simultaneous multiple authentications:

```
C3(rw)->set multiauth mode multi
```

clear multiauth mode

Use this command to clear the system authentication mode.

Syntax

```
clear multiauth mode
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the system authentication mode:

```
C3(rw)->clear multiauth mode
```

set multiauth precedence

Use this command to set the system's multiple authentication administrative precedence.

Syntax

set multiauth precedence {[**dot1x**] [**mac**] [**pwa**]}

Parameters

dot1x	Sets precedence for 802.1X authentication.
mac	Sets precedence for MAC authentication.
pwa	Sets precedence for port web authentication

Defaults

Default precedence order is dot1x, pwa, mac.

Mode

Switch command, read-write.

Usage

When a user is successfully authenticated by more than one method at the same time, the precedence of the authentication methods will determine which RADIUS-returned filter ID will be processed and result in an applied traffic policy profile.

Example

This example shows how to set precedence for MAC authentication:

```
C3(rw)->set multiauth precedence mac dot1x
```

clear multiauth precedence

Use this command to clear the system's multiple authentication administrative precedence to the default precedence order.

Syntax

clear multiauth precedence

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the multiple authentication precedence:

```
C3(rw)->clear multiauth precedence
```

show multiauth port

Use this command to display multiple authentication properties for one or more ports.

Syntax

show multiauth port [*port-string*]

Parameters

port-string	(Optional) Displays multiple authentication information for specific port(s).

Defaults

If port-string is not specified, multiple authentication information will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display multiple authentication information for ports ge.3.1-4. The number of "Max users" shown by this command varies depending on the platform.

```
C3(rw)->show multiauth port ge.3.1-4

Port          Mode         Max       Allowed    Current
                          users       users      users
------------ ------------ ---------- ---------- ----------
ge.3.1       auth-opt     n          1          0
ge.3.2       auth-opt     n          1          0
ge.3.3       auth-opt     n          1          0
ge.3.4       auth-opt     n          1          0
```

set multiauth port

Use this command to set multiple authentication properties for one or more ports.

Syntax

set multiauth port mode {**auth-opt** | **auth-reqd** | **force-auth** | **force-unauth**} | **numusers** *numusers port-string*

Parameters

mode **auth-opt** | **auth-reqd** | **force-auth** | **force-unauth**	Specifies the port(s)' multiple authentication mode as: • **auth-opt** — Authentication optional ("non-strict" behavior). If a user does not attempt to authenticate using 802.1x, or if 802.1x authentication fails, the port will allow traffic to be forwarded according to the defined default VLAN. • **auth-reqd** — Authentication is required. • **force-auth** — Authentication considered. • **force-unauth** — Authentication disabled.
numusers *numusers*	Specifies the number of users allowed authentication on port(s). Valid values depend on your specific platform. Refer to Appendix A, **Policy and Authentication Capacities** for information about multi-user capacities.
port-string	Specifies the port(s) on which to set multiple authentication properties.

Defaults

Default value for the number of users allowed to authenticate on a port is 1.

Mode

Switch command, read-write.

Examples

This example shows how to set the port multiple authentication mode to required on ge.3.14:

```
C3(rw)->set multiauth port mode auth-reqd ge.3.14
```

This example shows how to set the number of users allowed to authenticate on port ge.3.14 to 2:

```
C3(rw)->set multiauth port numusers 2 ge.3.14
```

clear multiauth port

Use this command to clear multiple authentication properties for one or more ports.

Syntax

clear multiauth port {**mode** | **numusers**} *port-string*

Parameters

mode	Clears the specified port's multiple authentication mode.
numusers	Clears the value set for the number of users allowed authentication on the specified port.
port-string	Specifies the port or ports on which to clear multiple authentication properties.

Defaults

None.

Mode

Switch command, read-write.

Examples

This example shows how to clear the port multiple authentication mode on port ge.3.14:

```
C3(rw)->clear multiauth port mode ge.3.14
```

This example shows how to clear the number of users on port ge.3.14:

```
C3(rw)->clear multiauth port numusers ge.3.14
```

show multiauth station

Use this command to display multiple authentication station (end user) entries.

Syntax

show multiauth station [**mac** *address*] [**port** *port-string*]

Parameters

mac *address*	(Optional) Displays multiple authentication station entries for a specific MAC address.
port *port-string*	(Optional) Displays multiple authentication station entries for one or more ports.

Mode

Switch command, read-only.

Defaults

If no options are specified, multiple authentication station entries will be displayed for all MAC addresses and ports.

Example

This example shows how to display multiple authentication station entries. In this case, two end user MAC addresses are shown:

```
C3(rw)->show multiauth station
Port         Address type  Address
------------ ------------  ------------------------
ge.1.20      mac           00-10-a4-9e-24-87
ge.2.16      mac           00-b0-d0-e5-0c-d0
```

show multiauth session

Use this command to display multiple authentication session entries.

Syntax

show multiauth session [**all**] [**agent** {**dot1x** | **mac** | **pwa**}] [**mac** *address*] [**port** *port-string*]

Parameters

all	(Optional) Displays information about all sessions, including those with terminated status.
agent dot1x | **mac** | **pwa**	(Optional) Displays 802.1X, or MAC, or port web authentication session information.
mac *address*	(Optional) Displays multiple authentication session entries for specific MAC address(es).
port *port-string*	(Optional) Displays multiple authentication session entries for the specified port or ports.

Defaults

If no options are specified, multiple authentication session entries will be displayed for all sessions, authentication types, MAC addresses, and ports.

Mode

Switch command, read-only.

Example

This example shows how to display multiple authentication session information for port ge.1.1.

```
C3(su)->show multiauth session port ge.1.1
_____________________________________________
Port             | ge.1.1            Station address   | 00-01-03-86-0A-87
Auth status      | success           Last attempt      | FRI MAY 18 11:16:36 2007
Agent type       | dot1x             Session applied   | true
Server type      | radius            VLAN-Tunnel-Attr  | none
Policy index     | 0                 Policy name       | Administrator
Session timeout  | 0                 Session duration  | 0,00:00:25
Idle timeout     | 5                 Idle time         | 0,00:00:00
Termination time | Not Terminated
```

show multiauth idle-timeout

Use this command to display the timeout value, in seconds, for an idle session for all authentication methods.

Syntax

show multiauth idle-timeout

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display timeout values for an idle session for all authentication types.

```
C3(su)->show multiauth idle-timeout
Authentication type  Timeout (sec)
-------------------- -------------
dot1x                0
pwa                  0
mac                  0
```

set multiauth idle-timeout

Use this command to set the maximum number of consecutive seconds an authenticated session may be idle before termination of the session.

Syntax

set multiauth idle-timeout [**dot1x** | **mac** | **pwa**] *timeout*

Parameters

dot1x	(Optional) Specifies the IEEE 802.1X port-based network access control authentication method for which to set the timeout value.
mac	(Optional) Specifies the Enterasys MAC authentication method for which to set the timeout value.
pwa	(Optional) Specifies the Enterasys Port Web Authentication method for which to set the timeout value.
timeout	Specifies the timeout value in seconds. The value can range from 0 to 65535. A value of 0 means that no idle timeout will be applied unless an idle timeout value is provided by the authenticating server.

Defaults

If no authentication method is specified, the idle timeout value is set for all authentication methods.

Mode

Switch mode, read-write.

Usage

If you set an idle timeout value, a MAC user whose MAC address has aged out of the forwarding database will be unauthenticated if no traffic has been seen from that address for the specified idle timeout period.

A value of zero indicates that no idle timeout will be applied unless an idle timeout value is provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may encode a Idle-Timeout Attribute in its authentication response.

Example

This example sets the idle timeout value for all authentication methods to 300 seconds.

```
C3(su)->set multiauth idle-timeout 300
```

clear multiauth idle-timeout

Use this command to reset the maximum number of consecutive seconds an authenticated session may be idle before termination of the session to its default value of 0.

Syntax

```
clear multiauth idle-timeout [dot1x | mac | pwa]
```

Parameters

dot1x	(Optional) Specifies the IEEE 802.1X port-based network access control authentication method for which to reset the timeout value to its default.
mac	(Optional) Specifies the Enterasys MAC authentication method for which to reset the timeout value to its default.
pwa	(Optional) Specifies the Enterasys Port Web Authentication method for which to reset the timeout value to its default.

Defaults

If no authentication method is specified, the idle timeout value is reset to its default value of 0 for all authentication methods.

Mode

Switch mode, read-write.

Example

This example resets the idle timeout value for all authentication methods to 0 seconds.

```
C3(su)->clear multiauth idle-timeout
```

show multiauth session-timeout

Use this command to display the session timeout value, in seconds, for all authentication methods.

Syntax

```
show multiauth session-timeout
```

Parameters

None.

Defaults

None.

Mode

Switch mode, read-only.

Example

This example displays the session timeout values for all authentication methods.

```
C3(su)->show multiauth session-timeout
Authentication type  Timeout (sec)
-------------------- -------------
dot1x                0
pwa                  0
mac                  0
```

set multiauth session-timeout

Use this command to set the maximum number of seconds an authenticated session may last before termination of the session.

Syntax

set multiauth session-timeout [**dot1x** | **mac** | **pwa**] *timeout*

Parameters

dot1x	(Optional) Specifies the IEEE 802.1X port-based network access control authentication method for which to set the session timeout value.
mac	(Optional) Specifies the Enterasys MAC authentication method for which to set the session timeout value.
pwa	(Optional) Specifies the Enterasys Port Web Authentication method for which to set the session timeout value.
timeout	Specifies the timeout value in seconds. The value can range from 0 to 65535. A value of 0 means that no session timeout will be applied unless a session timeout value is provided by the authenticating server.

Defaults

If no authentication method is specified, the session timeout value is set for all authentication methods.

Mode

Switch mode, read-write.

Usage

A value of zero may be superseded by a session timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may encode a Session-Timeout Attribute in its authentication response.

Example

This example sets the session timeout value for the IEEE 802.1X authentication method to 300 seconds.

```
C3(su)->set multiauth session-timeout dot1x 300
```

clear multiauth session-timeout

Use this command to reset the maximum number of consecutive seconds an authenticated session may last before termination of the session to its default value of 0.

Syntax

```
clear multiauth session-timeout [dot1x | mac | pwa]
```

Parameters

dot1x	(Optional) Specifies the IEEE 802.1X port-based network access control authentication method for which to reset the timeout value to its default.
mac	(Optional) Specifies the Enterasys MAC authentication method for which to reset the timeout value to its default.
pwa	(Optional) Specifies the Enterasys Port Web Authentication method for which to reset the timeout value to its default.

Defaults

If no authentication method is specified, the session timeout value is reset to its default value of 0 for all authentication methods.

Mode

Switch mode, read-write.

Example

This example resets the session timeout value for the IEEE 802.1X authentication method to 0 seconds.

```
C3(su)->clear multiauth session-timeout dot1x
```

Configuring User + IP Phone Authentication

User + IP phone authentication is a legacy feature that allows a user and their IP phone to both use a single port on the `switch` but to have separate policy roles. The user's PC and their IP phone are daisy-chained together with a single connection to the network.

This special application of multi-user authentication was inherited from legacy platforms (such as the B2 and C2) that could not natively support multiple users per port. The SecureStack C3 can support multiple users per port so the User + IP phone application should only be used if you are integrating SecureStack C3s into a legacy deployment.

With "User + IP Phone" authentication, the policy role for the IP phone is statically mapped using a policy admin rule which assigns any packets received with a VLAN tag set to a specific VID (for example, Voice VLAN) to an specified policy role (for example, IP Phone policy role). Therefore, it is required that the IP phone be configured to send VLAN-tagged packets tagged for the "Voice" VLAN. Refer to the **Usage** section for the command "set policy rule" on page 11-10 for additional information about configuring a policy admin rule that maps a VLAN tag to a policy role.

Note that if the IP phone authenticates to the network, the RADIUS accept message must return null values for RFC 3580 tunnel attributes and the Filter-ID.

The second policy role, for the user, can either be statically configured with the default policy role on the port or dynamically assigned through authentication to the network (using a RADIUS Filter-ID). When the default policy role is assigned on a port, the VLAN set as the port's PVID is mapped to the default policy role. When a policy role is dynamically applied to a user as the result of a successfully authenticated session, the “authenticated VLAN” is mapped to the policy role set in the Filter-ID returned from the RADIUS server. The “authenticated VLAN” may either be the PVID of the port, if the PVID Override for the policy profile is disabled, or the VLAN specified in the PVID Override if the PVID Override is enabled.

Configuring VLAN Authorization (RFC 3580)

Purpose

RFC 3580 Tunnel Attributes provide a mechanism to contain an 802.1X, MAC, or PWA authenticated user to a VLAN regardless of the PVID. This is referred to as dynamic VLAN assignment.

Please see section 3-31 of RFC 3580 for details on configuring a RADIUS server to return the desired tunnel attributes. As stated in RFC 3580, “... it may be desirable to allow a port to be placed into a particular Virtual LAN (VLAN), defined in [IEEE8021Q], based on the result of the authentication.”

The RADIUS server typically indicates the desired VLAN by including tunnel attributes within its Access-Accept parameters. However, the IEEE 802.1X or MAC authenticator can also be configured to instruct the VLAN to be assigned to the supplicant by including tunnel attributes within Access-Request parameters.

The following tunnel attributes are used in VLAN authorization assignment:

- Tunnel-Type - VLAN (13)
- Tunnel-Medium-Type - 802
- Tunnel-Private-Group-ID - VLANID

In order to authenticate RFC 3580 users, policy maptable response must be set to **tunnel** as described in “Configuring Policy Maptable Response” on page 26-52.

Note: A policy license, if applicable, is not required to deploy RFC 3580 dynamic VLAN assignment.

Commands

For information about...	Refer to page...
set vlanauthorization	26-50
set vlanauthorization egress	26-50
clear vlanauthorization	26-51
show vlanauthorization	26-51

set vlanauthorization

Enable or disable the use of the RADIUS VLAN tunnel attribute to put a port into a particular VLAN based on the result of authentication.

Syntax

set vlanauthorization {**enable** | **disable**} [*port-string*]

Parameters

enable | **disable**	Enables or disables vlan authorization/tunnel attributes.
port-string	(Optional) Specifies which ports to enable or disable the use of VLAN tunnel attributes/authorization. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

VLAN authentication is disabled by default.

Mode

Switch command, read-write.

Examples

This example shows how to enable VLAN authentication for all Gigabit Ethernet ports:

```
C3(rw)-> set vlanauthorization enable ge.*.*
```

This example shows how to disable VLAN authentication for all Gigabit Ethernet ports on switch unit/module 3:

```
C3(rw)-> set vlanauthorization disable ge.3.*
```

set vlanauthorization egress

Controls the modification of the current VLAN egress list of 802.1x authenticated ports for the VLANs returned in the RADIUS authorization filter id string.

Syntax

set vlanauthorization egress {**none** | **tagged** | **untagged**} *port-string*

Parameters

none	Specifies that no egress manipulation will be made.
tagged	Specifies that the authenticating port will be added to the current tagged egress for the VLAN-ID returned.
untagged	Specifies that the authenticating port will be added to the current untagged egress for the VLAN-ID returned (default).
port-string	Specifies that the port or list of ports. to which this command will apply. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

By default, administrative egress is set to untagged.

Mode

Switch command, read-write.

Example

This example shows how to enable the insertion of the RADIUS assigned VLAN to an 802.1q tag for all outbound frames for ports 10 through 15 on unit/module number 3.

```
C3(rw)->set vlanauthorization egress tagged ge.3.10-15
```

clear vlanauthorization

Use this command to return port(s) to the default configuration of VLAN authorization disabled, egress untagged.

Syntax

clear vlanauthorization [*port-string*]

Parameters

port-string	(Optional) Specifies which ports are to be restored to default configuration. If no port string is entered, the action will be a global setting. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If no port string is entered, all ports a will be reset to default configuration with VLAN authorization disabled and egress frames untagged.

Mode

Switch command, read-write.

Example

This example show how to clear VLAN authorization for all ports on slots 3, 4, and 5:

```
C3(rw)->clear vlanauthorization ge.3-5.*
```

show vlanauthorization

Displays the VLAN authentication status and configuration information for the specified ports.

Syntax

show vlanauthorization [*port-string*]

Parameters

port-string	(Optional) Displays VLAN authentication status for the specified ports. If no port string is entered, then the global status of the setting is displayed. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If no port string is entered, the status for all ports will be displayed.

Mode

Switch command, read-only.

Example

This command shows how to display VLAN authorization status for ge.1.1:

```
C3(su)->show vlanauthorization ge.1.1
Vlan Authorization:  - enabled
port     status   administrative   operational   authenticated     vlan id
                     egress          egress     mac address
-------  --------  -------------   -----------  -----------------  -------
 ge.1.1   enabled   untagged
```

Table 26-5 provides an explanation of command output. For details on enabling and assigning protocol and egress attributes, refer to "set vlanauthorization" on page 26-50 and "set vlanauthorization egress" on page 26-50.

Table 26-5 show vlanauthorization Output Details

Output Field	What It Displays...
port	Port identification
status	Port status as assigned by set vlanauthorization command
administrative egress	Port status as assigned by the set vlanauthorization egress command
operational egress	Port operational status of vlanauthorization egress.
authenticated mac address	If authentication has succeeded, displays the MAC address assigned for egress.
vlan id	If authentication has succeeded, displays the assigned VLAN id for ingress.

Configuring Policy Maptable Response

The policy maptable response feature allows you to define how the system should handle allowing an authenticated user onto a port based on the contents of the RADIUS server Access-Accept reply. There are three possible response settings: tunnel mode, policy mode, or both tunnel and policy, also known as hybrid authentication mode.

When the maptable response is set to **tunnel mode**, the system will use the tunnel attributes in the RADIUS reply to apply a VLAN to the authenticating user and will ignore any Filter-ID attributes in the RADIUS reply. On this platform, when tunnel mode is configured, no VLAN-to-policy mapping will occur. When using VLAN authorization, the policy maptable response should be set to tunnel (see "Configuring VLAN Authorization (RFC 3580)" on page 26-49).

When the maptable response is set to **policy mode**, the system will use the Filter-ID attributes in the RADIUS reply to apply a policy to the authenticating user and will ignore any tunnel attributes in the RADIUS reply. On this platform, when policy mode is configured, no VLAN-to-policy mapping will occur.

When the maptable response is set to **both**, or hybrid authentication mode, both Filter-ID attributes (dynamic policy assignment) and tunnel attributes (dynamic VLAN assignment) sent in RADIUS server Access-Accept replies are used to determine how the switch should handle authenticating users. On this platform, when hybrid authentication mode is configured, VLAN-to-policy mapping can occur, as described below in "When Policy Maptable Response is "Both"" on page 26-53.

Using hybrid authentication mode eliminates the dependency on having to assign VLANs through policy roles — VLANs can be assigned by means of the tunnel attributes while policy roles can be assigned by means of the Filter-ID attributes. Alternatively, VLAN-to-policy mapping can be used to map policies to users using the VLAN specified by the tunnel attributes, without having to configure Filter-ID attributes on the RADIUS server. This separation gives administrators more flexibility in segmenting their networks beyond the platform's hardware policy role limits.

Refer to "RADIUS Filter-ID Attribute and Dynamic Policy Profile Assignment" on page 26-3 for more information about Filter-ID attributes and "Configuring VLAN Authorization (RFC 3580)" on page 26-49 for more information about tunnel attributes.

Operational Description

When Policy Maptable Response is "Both"

Hybrid authentication mode uses both Filter-ID attributes and tunnel attributes. To enable hybrid authentication mode, use the set policy maptable command and set the **response** parameter to **both**. When configured to use both sets of attributes:

- If both the Filter-ID and tunnel attributes are present in the RADIUS reply, then the policy profile specified by the Filter-ID is applied to the authenticating user, and if VLAN authorization is enabled globally and on the authenticating user's port, the VLAN specified by the tunnel attributes is applied to the authenticating user.

  If VLAN authorization is not enabled, the VLAN specified by the policy profile is applied. See "Configuring VLAN Authorization (RFC 3580)" on page 26-49 for information about enabling VLAN authorization globally and on specific ports.

- If the Filter-ID attributes are present but the tunnel attributes are not present, the policy profile specified by the Filter-ID is applied, along with the VLAN specified by the policy profile.

- If the tunnel attributes are present but the Filter-ID attributes are not present or are invalid, and if VLAN authorization is enabled globally and on the authenticating user's port, then the switch will check the VLAN-to-policy mapping table (configured with the **set policy maptable** command):

  – If an entry mapping the received VLAN ID to a valid policy profile is found, then that policy profile, along with the VLAN specified by the policy profile, will be applied to the authenticating user.

  – If no matching mapping table entry is found, the VLAN specified by the tunnel attributes will be applied to the authenticating user.

  – If the VLAN-to-policy mapping table is invalid, then the etsysPolicyRFC3580MapInvalidMapping MIB is incremented and the VLAN specified by the tunnel attributes will be applied to the authenticating user.

If VLAN authorization is not enabled, the tunnel attributes are ignored.

When Policy Maptable Response is “Policy”

When the switch is configured to use only Filter-ID attributes, by setting the **set policy maptable** command **response** parameter to **policy**:

- If the Filter-ID attributes are present, the specified policy profile will be applied to the authenticating user. If no Filter-ID attributes are present, or if the policy ID is unknown or invalid, the default policy (if it exists) will be applied.
- If the tunnel attributes are present, they are ignored. No VLAN-to-policy mapping will occur.

On switches that support policy, the default maptable response mode is **policy**. On switches that do not support policy, the default maptable response mode is **tunnel**.

When Policy Maptable Response is “Tunnel”

When the switch is configured to use only tunnel attributes, by setting the **set policy maptable** command **response** parameter to **tunnel**, and if VLAN authorization is enabled both globally and on the authenticating user’s port:

- If the tunnel attributes are present, the specified VLAN will be applied to the authenticating user. No VLAN-to-policy mapping will occur.
- If the tunnel attributes are not present, the default policy VLAN will be applied if it exists. Otherwise, the port VLAN will be applied.
- If the Filter-ID attributes are present, they are ignored.

If VLAN authorization is not enabled, the user will be allowed onto the port with the default policy, if it exists. If no default policy exists, the port VLAN will be applied.

On switches that support policy, the default maptable response mode is **policy**. On switches that do not support policy, the default maptable response mode is **tunnel**.

Commands

For information about...	Refer to page...
show policy maptable	26-54
set policy maptable	26-55
clear policy maptable	26-56

show policy maptable

Use this command to display information about the current VLAN-to-policy mapping table and the switch’s policy maptable response setting.

Syntax

show policy maptable [*vlan-list*]

Parameters

vlan-list	(Optional) Specifies the VLAN or list of VLANs for which to display the VLAN-to-policy settings.

Defaults

If no VLAN list is specified, all entries in the VLAN-to-policy mapping table are displayed.

Mode

Switch command, read-only.

Usage

This command displays both the policy maptable response setting, and the entries in the VLAN-to-policy mapping table for one or multiple VLANs. Refer to "Operational Description" on page 26-53 for information about how the VLAN-to-policy mapping table is used.

Example

This example shows how to display the policy maptable response and all the entries in the VLAN-to-policy mapping table. In this example, hybrid authentication mode is enabled (because the policy maptable response is **both**).

```
C3(rw)->show policy maptable
Policy map response     :  both
Policy map last change  :  1 days 00:23:57

        VLAN ID        Policy Profile
        144            4               (Students)
        160            7               (Faculty)
```

set policy maptable

Use this command to configure the VLAN-to-policy mapping table and also the switch's maptable response setting— that is, whether the switch is in tunnel mode, policy mode, or hybrid authentication mode.

Syntax

set policy maptable {*vlan-list policy-index* | **response** {**both** | **policy** | **tunnel**}}

Parameters

vlan-list policy-index	Specifies an entry in the VLAN-to-policy mapping table, which relates a policy profile with a VLAN ID or range of IDs. *vlan-list* can range from 1 to 4093. *policy-index* can range from 1 to 1023.
response	Indicates that this command is configuring the policy maptable response.
both	Sets the maptable response to look at both the Filter-ID and tunnel attributes in a RADIUS Access-Accept reply to determine how to handle an authenticating user. This is equivalent to enabling hybrid authentication mode.
policy	Sets the maptable response to policy mode. The system will look at only the Filter-ID attributes in a RADIUS Access-Accept reply to determine how to handle an authenticating user.
tunnel	Sets the maptable response to tunnel mode. The system will look at only the tunnel attributes in a RADIUS Access-Accept reply to determine how to handle an authenticating user.

Defaults

No mapping table entries are configured.

The default policy maptable response setting is **policy** mode.

Mode

Switch command, read-write.

Usage

This command can be used to create entries in the VLAN-to-policy mapping table and also to set the switch's maptable response. Refer to "Operational Description" on page 26-53 for more information about the switch's operations for all maptable response parameters.

When you are using VLAN authorization for dynamic VLAN assignment, you should set the policy maptable response to **tunnel**. See "Configuring VLAN Authorization (RFC 3580)" on page 26-49.

Examples

This example shows how to set the policy maptable response to both, or hybrid authentication mode:

```
C3(rw)->set policy maptable response both
```

This example shows how to configure a policy mapping entry that will map VLAN 144 to policy profile 4.

```
C3(rw)->set policy maptable 144 4
```

clear policy maptable

Use this command to clear a VLAN-to-policy mapping table entry or to reset the maptable response to the default value of **policy** mode.

Syntax

clear policy maptable {*vlan-list* | **response**}

Parameters

vlan-list	Clears the policy profile mapping for the specified VLAN ID or range of VLANs.
response	Resets the maptable response to **policy**.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command can be used to remove an entry in the VLAN-to-policy mapping table or to change the maptable response back to the default value of **policy** mode.

Example

This example removes the entry in the mapping table for VLAN 144.

```
C3(rw)->show policy maptable
Policy map response     :  both
Policy map last change  :  1 days 17:23:57

        VLAN ID        Policy Profile
        144            4               (Students)
        160            7               (Faculty)

C3(rw)->clear policy maptable 144

C3(rw)->show policy maptable
Policy map response     :  both
Policy map last change  :  1 days 17:24:01

        VLAN ID        Policy Profile
        160            7               (Faculty)
```

Configuring MAC Locking

This feature locks a MAC address to one or more ports, preventing connection of unauthorized devices through the port(s). When source MAC addresses are received on specified ports, the switch discards all subsequent frames not containing the configured source addresses. The only frames forwarded on a “locked” port are those with the “locked” MAC address(es) for that port.

There are two methods of locking a MAC to a port: first arrival and static. The first arrival method is defined to be locking the first *n* number of MACs which arrive on a port configured with MAC locking enabled. The value *n* is configured with the **set maclock firstarrival** command.

The static method is defined to be statically provisioning a MAC-port lock using the **set maclock** command. The maximum number of static MAC addresses allowed for MAC locking on a port can be configured with the **set maclock static** command.

You can configure the switch to issue a violation trap if a packet arrives with a source MAC address different from any of the currently locked MAC addresses for that port.

MACs are unlocked as a result of:

- A link down event
- When MAC locking is disabled on a port
- When a MAC is aged out of the forwarding database when FirstArrival aging is enabled

When properly configured, MAC locking is an excellent security tool as it prevents MAC spoofing on configured ports. Also if a MAC were to be secured by something like Dragon Dynamic Intrusion Detection, MAC locking would make it more difficult for a hacker to send packets into the network because the hacker would have to change their MAC address and move to another port. In the meantime the system administrator would be receiving a maclock trap notification.

Purpose

To review, disable, enable, and configure MAC locking.

Commands

show maclock

Use this command to display the status of MAC locking on one or more ports.

Syntax

show maclock [*port-string*]

Parameters

port-string	(Optional) Displays MAC locking status for specified port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, MAC locking status will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display MAC locking information for ge.1.1.

```
C3(su)->show maclock ge.1.1
MAC locking is globally enabled

 Port      Port    Trap    Aging    Max Static  Max FirstArrival  Last Violating
Number   Status   Status   Status   Allocated     Allocated       MAC Address
```

```
-------  -------  -------- -------  ---------- ---------------  ---------------
ge.1.1   enabled  disabled  enabled  20         1                00:a0:c9:39:5c:b4
```

Table 26-6 provides an explanation of the command output.

Table 26-6 show maclock Output Details

Output Field	What It Displays...
Port Number	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
Port Status	Whether MAC locking is **enabled** or **disabled** on the port. MAC locking is globally disabled by default. For details on enabling MAC locking on the switch and on one or more ports, refer to "set maclock enable" on page 26-60 and "set maclock" on page 26-61.
Trap Status	Whether MAC lock trap messaging is **enabled** or **disabled** on the port. For details on setting this status, refer to "set maclock trap" on page 26-67.
Aging Status	Whether aging of FirstArrival MAC addresses is **enabled** or **disabled** on the port. Refer to "set maclock agefirstarrival" on page 26-65.
Max Static Allocated	The maximum static MAC addresses allowed locked to the port. For details on setting this value, refer to "set maclock static" on page 26-63.
Max FirstArrival Allocated	The maximum end station MAC addresses allowed locked to the port. For details on setting this value, refer to "set maclock firstarrival" on page 26-64.
Last Violating MAC Address	Most recent MAC address(es) violating the maximum static and first arrival value(s) set for the port.

show maclock stations

Use this command to display MAC locking information about end stations connected to the switch.

Syntax

```
show maclock stations [firstarrival | static] [port-string]
```

Parameters

firstarrival	(Optional) Displays MAC locking information about end stations first connected to MAC locked ports.
static	(Optional) Displays MAC locking information about static (management defined) end stations connected to MAC locked ports.
port-string	(Optional) Displays end station information for specified port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If no parameters are specified, MAC locking information will be displayed for all end stations.

Mode

Switch command, read-only.

Example

This example shows how to display MAC locking information for the end stations connected to all Gigabit Ethernet ports in unit/module 2:

```
C3(su)->show maclock stations ge.2.*
 Port Number  MAC Address          Status         State          Aging
 ------------ -----------------    -------------- -------------- -----
 ge.2.1       00:a0:c9:39:5c:b4    active         first arrival  true
 ge.2.7       00:a0:c9:39:1f:11    active         static         false
```

Table 26-7 provides an explanation of the command output.

Table 26-7 show maclock stations Output Details

Output Field	What It Displays...
Port Number	Port designation. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
MAC address	MAC address of the end station(s) locked to the port.
Status	Whether the end stations are **active** or **inactive**.
State	Whether the end station locked to the port is a **first arrival** or **static** connection.
Aging	When true, FirstArrival MACs that have aged out of the forwarding database will be removed for the associated port lock.

set maclock enable

Use this command to enable MAC locking globally or on one or more ports.

Note: MAC locking needs to be enabled globally and on appropriate ports for it to function.

Syntax

set maclock enable [*port-string*]

Parameters

port-string	(Optional) Enables MAC locking on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, MAC locking will be enabled globally.

Mode

Switch command, read-write.

Usage

When enabled and configured, MAC locking defines which MAC addresses, as well as how many MAC addresses are permitted to use specific port(s).

MAC locking is disabled by default at device startup. Configuring one or more ports for MAC locking requires globally enabling it on the device and then enabling it on the desired ports.

Example

This example shows how to enable MAC locking on ge.2.3:

```
C3(su)->set maclock enable ge.2.3
```

set maclock disable

Use this command to disable MAC locking globally or on one or more ports.

Syntax

set maclock disable [*port-string*]

Parameters

port-string	(Optional) Disables MAC locking on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, MAC locking will be disabled globally on the switch.

Mode

Switch command, read-write.

Example

This example shows how to disable MAC locking on ge.2.3:

```
C3(su)->set maclock disable ge.2.3
```

set maclock

Use this command to create a static MAC address-to-port locking, and to enable or disable MAC locking for the specified MAC address and port.

Syntax

set maclock *mac-address port-string* {**create** | **enable** | **disable**}

Parameters

mac-address	Specifies the MAC address for which MAC locking will be created, enabled or disabled.
port-string	Specifies the port on which to create, enable or disable MAC locking for the specified MAC. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

create	Establishes a MAC locking association between the specified MAC address and port. Create automatically enables MAC locking between the specified MAC address and port.
enable | **disable**	Enables or disables MAC locking between the specified MAC address and port.

Defaults

None.

Mode

Switch command, read-write.

Usage

Configuring a port for MAC locking requires globally enabling it on the switch first using the **set maclock enable** command as described in "set maclock enable" on page 26-60.

Static MAC locking a user on multiple ports is not supported.

Statically MAC locked addresses will display in the **show mac** output (as described on page 14-22) as address type "other" and will not remove them on link down.

Example

This example shows how to create a MAC locking association between MAC address 0e-03-ef-d8-44-55 and port ge.3.2:

```
C3(rw)->set maclock 0e-03-ef-d8-44-55 ge.3.2 create
```

clear maclock

Use this command to remove a static MAC address to port locking entry.

Syntax

clear maclock *mac-address port-string*

Parameters

mac-address	Specifies the MAC address that will be removed from the list of static MACs allowed to communicate on the port.
port-string	Specifies the port on which to clear the MAC address. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Usage

The MAC address that is cleared will no longer be able to communicate on the port unless the first arrival limit has been set to a value greater than 0 and this limit has not yet been met.

For example, if user B's MAC is removed from the static MAC address list and the first arrival limit has been set to 0, then user B will not be able to communicate on the port. If user A's MAC is removed from the static MAC address list and the first arrival limit has been set to 10, but only has 7 entries, user A will become the 8th entry and allowed to communicate on the port.

Example

This example shows how to remove a MAC from the list of static MACs allowed to communicate on port ge.3.2:

```
C3(rw)->clear maclock 0e-03-ef-d8-44-55 ge.3.2
```

set maclock static

Use this command to set the maximum number of static MAC addresses allowed per port. Static MACs are administratively defined.

Syntax

set maclock static *port-string value*

Parameters

port-string	Specifies the port on which to set the maximum number of static MACs allowed. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
value	Specifies the maximum number of static MAC addresses allowed per port. Valid values are 0 to 20.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the maximum number of allowable static MACs to 2 on ge.3.1:

```
C3(rw)->set maclock static ge.3.1 2
```

clear maclock static

Use this command to reset the number of static MAC addresses allowed per port to the default value of 20.

Syntax

clear maclock static *port-string*

Parameters

port-string	Specifies the port on which to reset number of static MAC addresses allowed. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the number of allowable static MACs on ge.2.3:

```
C3(rw)->clear maclock static ge.2.3
```

set maclock firstarrival

Use this command to restrict MAC locking on a port to a maximum number of end station addresses first connected to that port.

Syntax

`set maclock firstarrival` *`port-string value`*

Parameters

port-string	Specifies the port on which to limit MAC locking. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
value	Specifies the number of first arrival end station MAC addresses to be allowed connections to the port. Valid values are **0** to **600**.

Defaults

None.

Mode

Switch command, read-write.

Usage

The maclock first arrival count resets when the link goes down. This feature is beneficial if you have roaming users—the first arrival count will be reset every time a user moves to another port, but will still protect against connecting multiple devices on a single port and will protect against MAC address spoofing.

Note: Setting a port's first arrival limit to 0 does not deny the first MAC address learned on the port from passing traffic.

Example

This example shows how to restrict MAC locking to 6 MAC addresses on ge.2.3:

```
C3(su)->set maclock firstarrival ge.2.3 6
```

clear maclock firstarrival

Use this command to reset the number of first arrival MAC addresses allowed per port to the default value of 600.

Syntax

clear maclock firstarrival *port-string*

Parameters

port-string	Specifies the port on which to reset the first arrival value. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset MAC first arrivals on ge.2.3:

```
C3(su)->clear maclock firstarrival ge.2.3
```

set maclock agefirstarrival

Use this command to enable or disable the aging of first arrival MAC addresses. When enabled, first arrival MAC addresses that are aged out of the forwarding database will be removed from the associated port MAC lock.

Syntax

set maclock agefirstarrival *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) on which to enable or disable first arrival aging. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
enable | **disable**	Enable or disable first arrival aging. By default, first arrival aging is disabled.

Defaults

None.

Mode

Switch mode, read-write.

Example

This example enables first arrival aging on port ge.1.1.

```
C3(su)-> set maclock agefirstarrival ge.1.1 enable
```

clear maclock agefirstarrival

Use this command to reset first arrival aging on one or more ports to its default state of disabled.

Syntax

clear maclock agefirstarrival *port-string*

Parameters

port-string	Specifies the port(s) on which to disable first arrival aging. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch mode, read-write.

Example

This example disables first arrival aging on port ge.1.1.

```
C3(su)-> clear maclock agefirstarrival ge.1.1 enable
```

set maclock move

Use this command to move all current first arrival MACs to static entries.

Syntax

set maclock move *port-string*

Parameters

port-string	Specifies the port on which MAC will be moved from first arrival MACs to static entries. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

None.

Mode

Switch command, read-write.

Usage

If there are more first arrival MACs than the allowed maximum static MACs, then only the latest first arrival MACs will be moved to static entries. For example, if you set the maximum number of static MACs to 2 with the **set maclock static** command, and then executed the **set maclock move** command, even though there were five MACs in the first arrival table, only the two most recent MAC entries would be moved to static entries.

Example

This example shows how to move all current first arrival MACs to static entries on ports ge.3.1-40:

```
C3(rw)->set maclock move ge.3.1-40
```

set maclock trap

Use this command to enable or disable MAC lock trap messaging.

Syntax

set maclock trap *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port on which MAC lock trap messaging will be enabled or disabled. For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.
enable | **disable**	Enables or disables MAC lock trap messaging.

Defaults

None.

Mode

Switch command, read-write.

Usage

When enabled, this feature authorizes the switch to send an SNMP trap message if an end station is connected that exceeds the maximum values configured using the **set maclock firstarrival** and **set maclock static** commands. Violating MAC addresses are dropped from the device's (or stack's) filtering database.

Example

This example shows how to enable MAC lock trap messaging on ge.2.3:

```
C3(su)->set maclock trap ge.2.3 enable
```

Configuring Port Web Authentication (PWA)

About PWA

PWA provides a way of authenticating users through a Web portal before allowing general access to the network.

To log on using PWA, the user makes a request through a web browser for the PWA web page or is automatically redirected to this login page after requesting a URL in a browser.

Depending upon the authenticated state of the user, a login page or a logout page will display. When a user submits username and password, the switch then authenticates the user via a preconfigured RADIUS server. If the login is successful, then the user will be granted full network access according to the user's policy configuration on the switch.

Purpose

To review, enable, disable, and configure Port Web Authentication (PWA).

Commands

show pwa

Use this command to display port web authentication information for one or more ports.

Syntax

show pwa [*port-string*]

Parameters

port-string	(Optional) Displays PWA information for specific port(s).

Defaults

If *port-string* is not specified, PWA information will be displayed for all ports.

Mode

Switch command, read-only.

Example

This example shows how to display PWA information for ge.2.1:

```
C3(su)->show pwa ge.2.1
PWA Status                  - enabled
PWA IP Address              - 192.168.62.99
PWA Protocol                - PAP
PWA Enhanced Mode           - N/A
PWA Logo                    - enabled
PWA Guest Networking Status - disabled
PWA Guest Name              - guest
PWA Redirect Time           - N/A

Port     Mode              AuthStatus      QuietPeriod  MaxReq
-------- ----------------  --------------  -----------  ---------
ge.2.1   disabled          disconnected    60           16
```

Table 26-8 provides an explanation of the command output.

Table 26-8 show pwa Output Details

Output Field	What It Displays...
PWA Status	Whether or not port web authentication is enabled or disabled. Default state of disabled can be changed using the **set pwa** command as described in "set pwa" on page 26-70.
PWA IP Address	IP address of the end station from which PWA will prevent network access until the user is authenticated. Set using the **set pwa ipaddress** command as described in "set pwa ipaddress" on page 26-73.
PWA Protocol	Whether PWA protocol is CHAP or PAP. Default setting of PAP can be changed using the **set pwa protocol** command as described in "set pwa protocol" on page 26-73.
PWA Enhanced Mode	Whether PWA enhanced mode is enabled or disabled. Default state of disabled can be changed using the set pwa enhancedmode command as described in "set pwa enhancedmode" on page 26-79.

Table 26-8 show pwa Output Details (Continued)

Output Field	What It Displays...
PWA Logo	Whether the Enterasys logo will be displayed or hidden at user login. Default state of enabled (displayed) can be changed using the **set pwa displaylogo** command as described in "set pwa displaylogo" on page 26-72.
PWA Guest Networking Status	Whether PWA guest user status is disabled or enabled with RADIUS or no authentication. Default state of disabled can be changed using the **set pwa gueststatus** command as described in "set pwa gueststatus" on page 26-75.
PWA Guest Name	Guest user name for PWA enhanced mode networking. Default value of "guest" can be changed using the **set pwa guestname** command as described in "set pwa guestname" on page 26-74.
PWA Guest Password	Guest user's password. Default value of an empty string can be changed using the **set pwa guestpassword** command as described in "set pwa guestpassword" on page 26-75.
PWA Redirect Time	Time in seconds after login success before the user is redirected to the PWA home page.
Port	PWA port designation.
Mode	Whether PWA is enabled or disabled on his port.
Auth Status	Whether or not the port state is disconnected, authenticating, authenticated, or held (authentication has failed).
Quiet Period	Amount of time a port will be in the held state after a user unsuccessfully attempts to log on to the network. Default value of 60 can be changed using the **set pwa quietperiod** command as described in "set pwa quietperiod" on page 26-76.
MaxReq	Maximum number of log on attempts allowed before transitioning the port to a held state. Default value of 2 can be changed using the **set pwa maxrequests** command as described in "set pwa maxrequest" on page 26-77.

set pwa

Use this command to enable or disable port web authentication.

Syntax

```
set pwa {enable | disable}
```

Parameters

enable | **disable**	Enables or disables port web authentication.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to enable port web authentication:

```
C3(su)->set pwa enable
```

show pwa banner

Use this command to display the port web authentication login banner string.

Syntax

show pwa banner

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display the PWA login banner:

```
C3(su)->show pwa banner
Welcome to Enterasys Networks
```

set pwa banner

Use this command to configure a string to be displayed as the PWA login banner.

Syntax

set pwa banner *string*

Parameters

string	Specifies the PWA login banner.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the PWA login banner to “Welcome to Enterasys Networks ”:

```
C3(su)->set pwa banner “Welcome to Enterasys Networks”
```

clear pwa banner

Use this command to reset the PWA login banner to a blank string.

Syntax

clear pwa banner

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to reset the PWA login banner to a blank string

```
C3(su)->clear pwa banner
```

set pwa displaylogo

Use this command to set the display options for the Enterasys Networks logo.

Syntax

set pwa displaylogo {**display** | **hide**}

Parameters

display | **hide**	Displays or hides the Enterasys Networks logo when the PWA website displays.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to hide the Enterasys Networks logo:

```
C3(su)->set pwa displaylogo hide
```

set pwa ipaddress

Use this command to set the PWA IP address. This is the IP address of the end station from which PWA will prevent network access until the user is authenticated.

Syntax

set pwa ipaddress *ip-address*

Parameters

ip-address	Specifies a globally unique IP address. This same value must be configured into every authenticating switch in the domain.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set a PWA IP address of 1.2.3.4:

```
C3(su)->set pwa ipaddress 1.2.3.4
```

set pwa protocol

Use this command to set the port web authentication protocol.

Syntax

set pwa protocol {**chap** | **pap**}

Parameters

chap | **pap**	Sets the PWA protocol to: • CHAP (PPP Challenge Handshake Protocol) - encrypts the username and password between the end-station and the switch port. • PAP (Password Authentication Protocol- does not provide any encryption between the end-station the switch port.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set a the PWA protocol to CHAP:

```
C3(su)->set pwa protocol chap
```

set pwa guestname

Use this command to set a guest user name for PWA networking. PWA will use this name to grant network access to guests without established login names and passwords.

Syntax

`set pwa guestname` *`name`*

Parameters

name	Specifies a guest user name.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to set the PWA guest user name to “guestuser”:

```
C3(su)->set pwa guestname guestuser
```

clear pwa guestname

Use this command to clear the PWA guest user name.

Syntax

`clear pwa guestname`

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to clear the PWA guest user name

```
C3(su)->clear pwa guestname
```

set pwa guestpassword

Use this command to set the guest user password for PWA networking.

Syntax

set pwa guestpassword

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Usage

PWA will use this password and the guest user name to grant network access to guests without established login names and passwords.

Example

This example shows how to set the PWA guest user password name:

```
C3(su)->set pwa guestpassword
Guest Password: *********
Retype Guest Password: *********
```

set pwa gueststatus

Use this command to enable or disable guest networking for port web authentication.

Syntax

set pwa gueststatus {**authnone** | **authradius** | **disable**}

Parameters

authnone	Enables guest networking with no authentication method.
authradius	Enables guest networking with RADIUS authentication. Upon successful authentication from RADIUS, PWA will apply the policy returned from RADIUS to the PWA port.
disable	Disables guest networking.

Defaults

None.

Mode

Switch command, read-write.

Usage

PWA will use a guest password and guest user name to grant network access with default policy privileges to users without established login names and passwords.

Example

This example shows how to enable PWA guest networking with RADIUS authentication:

```
C3(su)->set pwa guestnetworking authradius
```

set pwa initialize

Use this command to initialize a PWA port to its default unauthenticated state.

Syntax

set pwa initialize [*port-string*]

Parameters

port-string	(Optional) Initializes specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, all ports will be initialized.

Mode

Switch command, read-write.

Example

This example shows how to initialize ports ge.1.5-7:

```
C3(su)->set pwa initialize ge.1.5-7
```

set pwa quietperiod

Use this command to set the amount of time a port will remain in the held state after a user unsuccessfully attempts to log on to the network.

Syntax

set pwa quietperiod *time* [*port-string*]

Parameters

time	Specifies quiet time in seconds.
port-string	(Optional) Sets the quiet period for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, quiet period will be set for all ports.

Mode

Switch command, read-write.

Example

This example shows how to set the PWA quiet period to 30 seconds for ports ge.1.5-7:

```
C3(su)->set pwa quietperiod 30 ge.1.5-7
```

set pwa maxrequest

Use this command to set the maximum number of log on attempts allowed before transitioning the PWA port to a held state.

Syntax

set pwa maxrequests *requests* [*port-string*]

Parameters

maxrequests	Specifies the maximum number of log on attempts.
port-string	(Optional) Sets the maximum requests for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, maximum requests will be set for all ports.

Mode

Switch command, read-write.

Example

This example shows how to set the PWA maximum requests to 3 for all ports:

```
C3(su)->set pwa maxrequests 3
```

set pwa portcontrol

This command enables or disables PWA authentication on select ports.

Syntax

set pwa portcontrol {**enable** | **disable**} [*port-string*]

Parameters

enable | **disable**	Enables or disables PWA on specified ports.
port-string	(Optional) Sets the control mode on specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, PWA will enabled on all ports.

Mode

Switch command, read-write.

Example

This example shows how to enable PWA on ports 1-22:

```
C3(su)->set pwa portcontrol enable ge.1.1-22
```

show pwa session

Use this command to display information about current PWA sessions.

Syntax

show pwa session [*port-string*]

Parameters

port-string	(Optional) Displays PWA session information for specific port(s). For a detailed description of possible *port-string* values, refer to "Port String Syntax Used in the CLI" on page 7-1.

Defaults

If *port-string* is not specified, session information for all ports will be displayed.

Mode

Switch command, read-only.

Example

This example shows how to display PWA session information:

```
C3(su)->show pwa session
Port     MAC               IP              User          Duration     Status
-------- ----------------- --------------- ------------- ------------ ---------
ge.2.19  00-c0-4f-20-05-4b 172.50.15.121   pwachap10     0,14:46:55   active
ge.2.19  00-c0-4f-24-51-70 172.50.15.120   pwachap1      0,15:43:30   active
ge.2.19  00-00-f8-78-9c-a7 172.50.15.61    pwachap11     0,14:47:58   active
```

set pwa enhancedmode

This command enables PWA URL redirection. The switch intercepts all HTTP packets on port 80 from the end user, and sends the end user a refresh page destined for the PWA IP Address configured.

Syntax

set pwa enhancedmode {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables PWA **enhancedmode**.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to enable PWA **enhancedmode**:

```
C3(su)->set pwa enhancedmode enable
```

Configuring Secure Shell (SSH)

Purpose

To review, enable, disable, and configure the Secure Shell (SSH) protocol, which provides secure Telnet.

Commands

For information about...	Refer to page...
show ssh status	26-80
set ssh	26-80
set ssh hostkey	26-81

show ssh status

Use this command to display the current status of SSH on the switch.

Syntax

show ssh status

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example shows how to display SSH status on the switch:

```
C3(su)->show ssh status
 SSH Server status: Disabled
```

set ssh

Use this command to enable, disable or reinitialize SSH server on the switch. By default, the SSH server is disabled.

Syntax

set ssh {**enable** | **disable** | **reinitialize**}

Parameters

enable | disable	Enables or disables SSH, or reinitializes the SSH server.
reinitialize	Reinitializes the SSH server.

Defaults

None.

Mode

Switch command, read-write.

Example

This example shows how to disable SSH:

```
C3(su)->set ssh disable
```

set ssh hostkey

Use this command to reinitialize new SSH authentication keys.

Syntax

`set ssh hostkey reinitialize`

Parameters

reinitialize	Reinitializes the server host authentication keys.

Defaults

None

Mode

Switch command, read-write.

Example

This example shows how to regenerate SSH keys:

```
C3(su)->set ssh hostkey reinitialize
```

Configuring Access Lists

Router: These commands can be executed when the device is in **router mode** only. For details on how to enable router configuration modes, refer to “Enabling Router Configuration Modes” on page 18-2.

Note: Refer to the Release Notes for your product for any limitations that may apply to access control lists.

Purpose

To review and configure security access control lists (ACLs), which permit or deny access to routing interfaces based on protocol and IP address restrictions.

Commands

For information about...	Refer to page...
show access-lists	26-82
access-list (standard)	26-83
access-list (extended)	26-84
ip access-group	26-86

show access-lists

Use this command to display configured IP access lists when operating in router mode.

Syntax

show access-lists [*number*]

Parameters

access-list-number	(Optional) Displays access list information for a specific access list number. Valid values are between **1** and **199**.

Defaults

If *number* is not specified, the entire table of access lists will be displayed.

Mode

Any router mode.

Example

This example shows how to display IP access list number 145. This is an extended access list, which permits or denies ICMP, UDP and IP frames based on restrictions configured with one of the **access-list** commands. For details on configuring standard access lists, refer to “access-list (standard)” on page 26-83. For details on configuring extended access lists, refer to “access-list (extended)” on page 26-84.

```
C3(su)->router#show access-lists 145

Extended IP access list 145
   1: permit icmp host 88.255.255.254 any
   2: permit icmp any host 11.11.16.16
   3: deny icmp any any
   4: permit tcp host 88.255.255.254 any eq 22
   5: permit udp 88.255.128.0 0.0.127.255 eq 161 any
   6: permit tcp any host 230.10.230.10 eq 1234
   7: deny tcp any any eq 23
   8: permit ip 88.255.128.0 0.0.127.255 any
   9: deny ip any 224.0.0.0 31.0.0.0
```

access-list (standard)

Use this command to define a standard IP access list by number when operating in router mode. The **no** form of this command removes the defined access list or entry.

Syntax

To create an ACL entry:

access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]

no access-list *access-list-number* [*entryno* [*entryno*]]

To insert or replace an ACL entry:

access-list *access-list-number* **insert** | **replace** *entryno* {**deny** | **permit**} *source* [*source-wildcard*]

To move entries within an ACL:

access-list *access-list-number* **move** *destination source1* [*source2*]

Parameters

access-list-number [*entryno* [*entryno*]]	Specifies a standard access list number. Valid values are from **1** to **99.** When using the **no access-list** command, you can delete a whole access-list, or only specific entries in the list with the optional *entryno* parameter. Specify a range of entries by entering the start and end entry numbers.
deny | **permit**	Denies or permits access if specified conditions are met.
source	Specifies the network or host from which the packet will be sent. Valid options for expressing source are: • IP address or range of addresses (A.B.C.D) • **any** - Any source host • **host** *source* - IP address of a single source host
source-wildcard	(Optional) Specifies the bits to ignore in the *source* address.

insert | **replace** *entryno*	(Optional) Inserts this new entry before a specified entry in an existing ACL, or replaces a specified entry with this new entry.
move *destination source1 source2*	(Optional) Moves a sequence of access list entries before another entry. *Destination* is the number of the existing entry before which this new entry will be moved. *Source1* is a single entry number or the first entry number in the range to be moved. *Source2* (optional) is the last entry number in the range to be moved. If *source2* is not specified, only the *source1* entry will be moved.

Defaults

If **insert, replace** or **move** are not specified, the new entry will be appended to the access list.

If *source2* is not specified with **move**, only one entry will be moved.

Mode

Global configuration: C3(su)->router(Config)#

Usage

Valid access list numbers for standard ACLs are **1** to **99**. For extended ACLs, valid values are **100** to **199**.

Access lists are applied to interfaces by using the **ip access-group** command (page 26-86).

All access lists have an implicit "deny any any" statment as their last entry.

Examples

This example shows how to create access list 1 with three entries that allow access to only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list entries will be rejected:

```
C3(su)->router(Config)#access-list 1 permit 192.5.34.0 0.0.0.255
C3(su)->router(Config)#access-list 1 permit 128.88.0.0 0.0.255.255
C3(su)->router(Config)#access-list 1 permit 36.0.0.0 0.255.255.255
```

This example moves entry 16 to the beginning of ACL 22:

```
C3(su)->router(Config)#access-list 22 move 1 16
```

access-list (extended)

Use this command to define an extended IP access list by number when operating in router mode. The **no** form of this command removes the defined access list or entry:

Syntax

To create an extended ACL entry:

access-list *access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] [**eq** *port*] *destination* [*destination-wildcard*] [**eq** *port*]

no access-list *access-list-number* [*entryno* [*entryno*]]

To insert or replace an ACL entry:

access-list *access-list-number* **insert** | **replace** *entryno* {**deny** | **permit**} *protocol source* [*source-wildcard*] [**eq** *port*] *destination* [*destination-wildcard*] [**eq** *port*]

To move entries within an ACL:

access-list *access-list-number* **move** *destination source1* [*source2*]

Parameters

access-list-number [*entryno* [*entryno*]]	Specifies an extended access list number. Valid values are from **100** to **199**. When using the **no access-list** command, you can delete a whole access-list, or only specific entries in the list with the optional *entryno* parameter. Specify a range of entries by entering the start and end entry numbers.
deny | **permit**	Denies or permits access if specified conditions are met.
protocol	Specifies an IP protocol for which to deny or permit access. Valid values and their corresponding protocols are: • **ip -** Any Internet protocol • **udp -** User Datagram Protocol • **tcp** - Transmission Control Protocol • **icmp** - Internet Control Message Protocol
source	Specifies the network or host from which the packet will be sent. Valid options for expressing source are: • IP address or range of addresses (A.B.C.D) • **any** - Any source host • **host** *source* - IP address of a single source host
source-wildcard	(Optional) Specifies the bits to ignore in the *source* address.
eq *port*	(Optional) Applies access rules to TCP or UDP source and/or destination port numbers equal to the specified port number. Port numbers can range from 0 to 65535. **Note:** This parameter is not available when you specify the **icmp** protocol.
destination	Specifies the network or host to which the packet will be sent. Valid options for expressing destination are: • IP address (A.B.C.D) • **any** - Any destination host • **host** *source* - IP address of a single destination host
destination-wildcard	(Optional) Specifies the bits to ignore in the *destination* address.
insert | **replace** *entryno*	(Optional) Inserts this new entry before a specified entry in an existing ACL, or replaces a specified entry with this new entry.
move *destination source1 source2*	(Optional) Moves a sequence of access list entries before another entry. *Destination* is the number of the existing entry before which this new entry will be moved. *Source1* is a single entry number or the first entry number in the range to be moved. *Source2* (optional) is the last entry number in the range to be moved. If *source2* is not specified, only the *source1* entry will be moved.

Defaults

If **insert**, **replace, or move** are not specified, the new entry will be appended to the access list.

If *source2* is not specified with **move**, only one entry will be moved.

If **eq** *port* is not specified, TCP/UDP ports are not used for filtering. Only the protocol, source, and destination are used for applying the rule.

Mode

Global configuration: C3(su)->router(Config)#

Usage

Access lists are applied to interfaces by using the **ip access-group** command as described in "ip access-group" on page 26-86.

Valid *access-list-numbers* for extended ACLs are **100** to **199**. For standard ACLs, valid values are **1** to **99**.

All access lists have an implicit "deny any any" statment as their last entry.

Examples

This example shows how to define access list 145 to deny ICMP transmissions from any source and for any destination:

```
C3(su)->router(Config)#access-list 145 deny ICMP any any
```

This example appends to access list 145 a permit statement that allows the host with IP address 88.255.255.254 to do an SSH remote login to any destination on TCP port 22.

```
C3(su)->router(Config)#access-list 145 permit tcp host 88.255.255.254 any eq 22
```

This example appends to access list 145 a permit statement that allows SNMP control traffic (from UDP port 161) to be sent from IP addresses within the range defined by 88.255.128.0 0.0.127.255 to any destination.

```
C3(su)->router(Config)#access-list 145 permit udp 88.255.128.0 0.0.127.255 eq 161
any
```

ip access-group

Use this command to apply access restrictions to inbound frames on an interface when operating in router mode. The **no** form of this command removes the specified access list.

Syntax

ip access-group *access-list-number* **in**
no ip access-group *access-list-number* **in**

Parameters

access-list-number	Specifies the number of the access list to be applied to the access list. This is a decimal number from **1** to **199**.
in	Filters inbound frames.

Defaults

None.

Mode

Interface configuration: C3(su)->router(Config-if(Vlan <vlan_id>))#

Usage

ACLs must be applied per routing interface. An access list can be applied to inbound traffic only. Access lists can now be applied to routed VLANs which incorporate LAGs.

Example

This example shows how to apply access list 1 for all inbound frames on the VLAN 1 interface. Through the definition of access list 1, only frames with a source address on the 192.5.34.0/24 network will be routed. All the frames with other source addresses received on the VLAN 1 interface are dropped:

```
C3(su)->router(Config)#access-list 1 permit 192.5.34.0 0.0.0.255
C3(su)->router(Config)#interface vlan 1
C3(su)->router(Config-if(Vlan 1))#ip access-group 1 in
```

27

TACACS+ Configuration

This chapter provides information about the commands used to configure and monitor TACACS+ (Terminal Access Controller Access-Control System Plus).

TACACS+ is a security protcol that provides services for secure authentication, CLI command authorization, and CLI auditing for administrative access. It can be used as an alternative to the standard RADIUS security protocol (RFC 2865). TACACS+ runs over TCP and encrypts the body of each management packet.

Based on the now obsolete TACACS protocol (defined in RFC 1492), TACACS+ is defined in an un-published and expired Internet Draft draft-grant-tacacs-02.txt, "The TACACS+ Protocol Version 1.78," January, 1997.

For detailed information about using TACACS+ in your network, refer to the Enterasys Feature Guide "TACACS+ Configuration" located on the Enterasys web site:

http://www.enterasys.com/support/manuals/f.html#M

show tacacs

Use this command to display the current TACACS+ configuration information and status.

Syntax

show tacacs [**state**]

Parameters

state	(Optional) Displays only the TACACS+ client status.

Defaults

If **state** is not specified, all TACACS+ configuration information will be displayed.

Mode

Switch command, Read-Only.

Example

This example shows how to display all TACACS configuration information.

```
C3(ro)->show tacacs
TACACS+ status:Disabled
TACACS+ session accounting state:disable
TACACS+ command authorization state:disable
TACACS+ command auccounting state:disable
TACACS+ single connect state:Disabled
TACACS+ service: exec
TACACS+ session authorization A-V pairs:
        access-level    attribute    value
           read-only     priv-lvl     0
          read-write     priv-lvl     1
          super-user     priv-lvl    15
TACACS+ Server  IP address      Port    Timeout
--------------  ----------     ------   -------
1               192.168.10.1    49      10
```

Table 27-1 provides an explanation of the command output.

Table 27-1 show tacacs Output Details

Output...	What it displays...
TACACS+ status	Whether the TACACS+ client is **enabled** or **disabled**.
TACACS+ session accounting state	Whether TACACS+ session accounting is **enabled** or **disabled**.
TACACS+ command authorization state	Whether TACACS+ command authorization is **enabled** or **disabled**.
TACACS+ command accounting state	Whether TACACS+ command accounting is **enabled** or **disabled**.

Table 27-1 show tacacs Output Details (Continued)

Output...	What it displays...
TACACS+ singleconnect state	Whether TACACS+ singleconnect is **enabled** or **disabled**. When enabled, the TACACS+ client sends multiple requests over a single TCP connection.
TACACS+ service	The name of the service that is requested by the TACACS+ client for session authorization. “exec” is the default service name.
TACACS+ session authorization A-V pairs	Displays the attribute – value pairs that are mapped to the **read-only**, **read-write**, and **super-user** access privilege levels for the service requested for session authorization. The attribute names and values shown in the example above are the default values.
TACACS+ Server	Displays the TACACS+ server information used by the TACACS+ client.

set tacacs

Use this command to enable or disable the TACACS+ client.

Syntax

`set tacacs` {**`enable`** | **`disable`**}

Parameters

enable | **disable**	Enables or disables the TACACS client.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

The TACACS+ client can be enabled on the switch anytime, with or without a TACACS+ server online. If the TACACS+ server is offline and TACACS+ is enabled, the login authentication is switched to RADIUS or local, if enabled.

Examples

This example shows how to enable the TACACS+ client.

```
C3(rw)->set tacacs enable
```

show tacacs server

Use this command to display the current TACACS+ server configuration.

Syntax

`show tacacs server` {*`index`* | **`all`**}

Parameters

index	Display the configuration of the TACACS+ server identified by *index*. The value of *index* can range from 1 to 2,147,483,647.
all	Display the configuration for all configured TACACS+ servers.

Defaults

None.

Mode

Switch command, Read-Only.

Example

This example displays configuration information for TACACS+ server 1.

```
C3(ro)->show tacacs server 1
TACACS+ Server  IP address      Port    Timeout
--------------  ----------     ------   -------
1               192.168.10.1    49      10
```

set tacacs server

Use this command to configure the TACACS+ server(s) to be used by the TACACS+ client. You can configure the timeout value for all configured servers or a single server, or you can configure the IP address, TCP port, and secret for a single server. For simplicity, two syntax statements are shown.

Syntax

set tacacs server {**all** | *index*} **timeout** *seconds*

set tacacs server *index address port secret*

Parameters

all	Specify the timeout value for all configured TACACS+ servers.
index	Configure the TACACS+ server identified by *index*. The value of *index* can range from 1 to 2,147,483,647.
timeout *seconds*	Set the timeout value for the specified server(s) in seconds. The value of *seconds* can range from 1 to 180 seconds. The default timeout value is 10 seconds.
address	Specify the IP address of the TACACS+ server.
port	Specify the TCP port for the TACACS+ server. The value of *port* can range from 0 to 65535, but typically, port 49 is specified.
secret	Specify the secret (shared password) for the TACACS+ server.

Defaults

No TACACS+ servers are configured by default.

When you do configure a TACACS+ server, the default timeout value is 10 seconds.

Mode

Switch command, Read-Write.

Usage

Up to 5 TACACS+ servers can be configured, with the index value of 1 having the highest priority. If you want to change the default timeout value for a specific server or all servers, you must enter the command using the **timeout** parameter.

When at least one backup server has been configured and the switch loses contact with the primary server, the switch will contact the next server in priority. If the switch was trying to authenticate a user when the connection was lost, or if the default login access (read-only permissions) had been received, the switch will try to authenticate again.

If a user had already been authenticated and authorized, then the backup server is contacted without requiring any authentication. The backup server will just authorize or account for the packets coming in for that user. Since a task ID is associated with each accounting session, if there is a failover to a backup server, the accounting information will still be associated with the correct session using the task ID.

When a failover to a backup server occurs, syslog messages are generated containing the reason for the failure.

Example

This example configures TACACS+ server 1. Then, the default timeout value of 10 seconds is changed to 20 seconds.

```
C3(rw)->set tacacs server 1 192.168.10.10 49 mysecret
C3(rw)->set tacacs server 1 timeout 20
```

clear tacacs server

Use this command to remove one or all configured TACACS+ servers, or to return the timeout value to its default value for one or all configured TACACS+ servers.

Syntax

clear tacacs server {**all** | *index*} [**timeout**]

Parameters

all	Specifies that all configured TACACS+ servers should be affected.
index	Specifies one TACACS+ server to be affected.
timeout	(Optional) Return the timeout value to its default value of 10 seconds.

Defaults

If **timeout** is not specified, the affected TACACS+ servers will be removed.

Mode

Switch command, Read-Write.

Examples

This example removes TACACS+ server 1.

```
C3(rw)->clear tacacs server 1
```

This example resets the timeout value to its default value of 10 seconds for all configured TACACS+ servers.

```
C3(rw)->clear tacacs server all timeout
```

show tacacs session

Use this command to display the current TACACS+ client session settings.

Syntax

show tacacs session {**authorization** | **accounting**}

Parameters

authorization	Display client session authorization settings.
accounting	Display client session accounting settings.

Defaults

None.

Mode

Switch command, Read-Only.

Examples

This example shows how to display client session authorization information:

```
C3(ro)->show tacacs session authorization
TACACS+ service: exec
TACACS+ session authorization A-V pairs:
        access-level    attribute    value
        read-only       priv-lvl     0
        read-write      priv-lvl     1
        super-user      priv-lvl     15
```

This example shows how to display client session accounting state.

```
C3(ro)->show tacacs session accounting
 TACACS+ session accounting state:  enabled
```

set tacacs session

Use this command to enable or disable TACACS+ session accounting, or to configure TACACS+ session authorization parameters. For simplicity, separate syntax formats are shown for configuring session accounting and session authorization.

Syntax

```
set tacacs session accounting {enable | disable}
set tacacs session authorization {service name | read-only attribute value |
read-write attribute value | super-user attribute value}
```

Parameters

accounting	Specifies that TACACS+ session accounting is being configured.
enable | **disable**	Enables or disables TACACS+ session accounting.
authorization	Specifies that TACACS+ session authorization is being configured.
service *name*	Specifies the name of the service that the TACACS+ client will request from the TACACS+ server. The *name* specified here must match the name of a service configured on the server. The default service name is exec.
read-only *attribute value*	Specifies that the **read-only** access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by *attribute* and *value*. By default, *attribute* is "priv-lvl" and *value* is 0.
read-write *attribute value*	Specifies that the **read-write** access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by *attribute* and *value*. By default, *attribute* is "priv-lvl" and *value* is 1.
super-user *attribute value*	Specifies that the **super-user** access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by *attribute* and *value*. By default, *attribute* is "priv-lvl" and *value* is 15.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

When session accounting is enabled, the TACACS+ server will log accounting information, such as start and stop times, IP address of the client, and so forth, for each authorized client session.

When the TACACS+ client is enabled on the switch (with the **set tacacs enable** command), the session authorization parameters configured with this command are sent by the client to the TACACS+ server when a session is initiated on the switch. The parameter values must match a service and access level attribute-value pairs configured on the server for the session to be authorized. If the parameter values do not match, the session will not be allowed.

The service name and attribute-value pairs can be any character string, and are determined by your TACACS+ server configuration.

Since a task ID is associated with each accounting session, if there is a failover to a backup server, the accounting information will still be associated with the correct session using the task ID.

Examples

This example configures the service requested by the TACACS+ client as the service name "basic."

```
C3(rw)->set tacacs session authorization service basic
```

This example maps the **read-write** access privilege level to an attribute named "priv-lvl" with the value of 5 configured on the TACACS+ server.

```
C3(rw)->set tacacs session authorization read-write priv-lvl 5
```

This example enables TACACS+ session accounting.

```
C3(rw)->set tacacs session accounting enable
```

clear tacacs session

Use this command to return the TACACS+ session authorization settings to their default values.

Syntax

clear tacacs session authorization {[**service**]|[**read-only**]|[**read-write**] | [**super-user**]}

Parameters

authorization	Clears the TACACS+ session authorization parameters.
service	Clears the TACACS+ session authorization service name to the default value of "exec."
read-only	Clears the TACACS+ session authorization read-only attribute-value pair to their default values of "priv-lvl" and 0.
read-write	Clears the TACACS+ session authorization read-write attribute-value pair to their default values of "priv-lvl" and 1.
super-user	Clears the TACACS+ session authorization super-user attribute-value pair to their default values of "priv-lvl" and 15.

Defaults

At least one of the session authorization parameters must be specified.

Mode

Switch command, Read-Write.

Examples

This example shows how to return the service name to the default of "exec."

```
C3(rw)->clear tacacs session authorization service
```

This example shows how to return all the session authorization parameters to their default values.

```
C3(rw)->clear tacacs session authorization service read-only read-write super-
user
```

show tacacs command

Use this command to display the status (enabled or disabled) of TACACS+ accounting or authorization on a per-command basis.

Syntax

show tacacs command {**accounting** | **authorization**}

Parameters

accounting	Display the status of TACACS+ accounting on a per-command basis.
authorization	Display the status of TACACS+ authorization on a per-command basis.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to display the state of the TACACS+ client's command authorization.

```
C3(rw)->show tacacs command authorization
TACACS+ command authorization state:  enabled
```

set tacacs command

Use this command to enable or disable TACACS+ accounting or authorization on a per-command basis.

Syntax

set tacacs command {**accounting** | **authorization**} {**enable** | **disable**}

Parameters

accounting | **authorization**	Specifies either TACACS+ accounting or authorization to be enabled or disabled.
enable | **disable**	Enable or disable accounting or authorization on a per-command basis.

Defaults

None.

Mode

Switch command, Read-Write.

Usage

In order for per-command accounting or authorization by a TACACS+ server to take place, the command must be executed within an authorized session.

When per-command accounting is enabled, the TACACS+ server will log accounting information, such as start and stop times, IP address of the client, and so forth, for each command executed during the session.

When per-command authorization is enabled, the TACACS+ server will check whether each command is permitted for that authorized session and return a success or fail. If the authorization fails, the command is not executed.

Example

This example shows how to enable TACACS+ authorization on a command basis.

```
C3(rw)->set tacacs command authorization enable
```

show tacacs singleconnect

Use this command to display the current status of the TACACS+ client's ability to send multiple requests over a single TCP connection.

Syntax

```
show tacacs singleconnect
```

Parameters

None.

Defaults

None.

Mode

Switch command, Read-Write.

Example

This example shows how to display the state of the TACACS+ client's ability to send multiple requests over a single connection.

```
C3(rw)->show tacacs singleconnect
  TACACS+ single-connect state:  enabled
```

set tacacs singleconnect

Use this command to enable or disable the ability of the TACACS+ client to send multiple requests over a single TCP connection. When enabled, the TACACS+ client will use a single TCP connection for all requests to a given TACACS+ server.

Syntax

```
set tacacs singleconnect {enable | disable}
```

Parameters

enable | **disable**	Enable or disable the ability to send multiple requests over a single TCP connection.

Defaults

None.

Mode

Switch command, Read-Write.

Examples

This example shows how to disable sending multiple requests over a single connection.

```
C3(rw)->set tacacs singleconnect disable
```

show tacacs interface

Use this command to display the interface used for the source IP address of the TACACS+ packets generated by the switch.

Syntax

show tacacs interface

Parameters

None.

Defaults

None.

Mode

Switch mode, read-only.

Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the TACACS+ packets generated by the switch.

```
C3(rw)->show tacacs interface
loopback 1  192.168.10.1
```

set tacacs interface

Use this command to specify the interface used for the source IP address of the TACACS+ packets generated by the switch.

Syntax

set tacacs interface {**loopback** *loop-ID* | **vlan** *vlan-ID*}

Parameters

loopback *loop-ID*	Specifies the loopback interface to be used. The value of *loop-ID* can range from 0 to 7.

vlan *vlan-ID*	Specifies the VLAN interface to be used. The value of vlan-ID can range from 1 to 4093.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command allows you to configure the source IP address used by the TACACS+ application on the switch when generating packets for management purposes. Any of the management interfaces, including VLAN routing interfaces, can be configured as the source IP address used in packets generated by the TACACS+ client.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the IP address of the Host interface will be used.

If a non-loopback interface is configured with this command, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the TACACS+ client source IP address.

```
C3(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
C3(rw)->router(Config-if(Vlan 100))#exit
C3(rw)->router(Config)#exit
C3(rw)->router#exit
C3(rw)->router>exit
C3(rw)->set tacacs interface vlan 100

C3(rw)->show tacacs interface
vlan 100  192.168.10.1
```

clear tacacs interface

Use this command to clear the interface used for the source IP address of the TACACS+ client back to the default of the Host interface.

Syntax

```
clear tacacs interface
```

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This command returns the interface used for the source IP address of the TACACS+ client back to the default of the Host interface.

```
C3(rw)->show tacacs interface
vlan 100  192.168.10.1
C3(rw)->clear tacacs interface
C3(rw)->
```

28

sFlow Configuration

This chapter provides information about the commands used to configure and monitor the sFlow system.

Overview

sFlow is a method for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives visibility into network activity, enabling effective management and control of network resources.

An sFlow solution consists of an sFlow Agent, embedded in the network device such as a switch or router, and an sFlow Collector. The sFlow Agent uses sampling technology to capture traffic statistics from the device it is monitoring and immediately forwards the sampled traffic statistics to an sFlow Collector for analysis in sFlow datagrams.

The sFlow Agent uses two forms of sampling— statistical packet-based sampling of switched or routed Packet Flows, and time-based sampling of counters.

Version 5 of sFlow is described in detail in the document entitled “sFlow Version 5” available from sFlow.org (http://www.sflow.org).

Using sFlow in Your Network

The advantages of using sFlow include:

- sFlow makes it possible to monitor ports of a switch, with no impact on the distributed switching performance. (See “Usage Notes” on page 28-3 for more information.)
- sFlow requires very little memory or CPU usage. Samples are not aggregated into a flow-table on the switch — they are forwarded immediately over the network to the sFlow Collector.
- The system is tolerant to packet loss in the network. (The statistical model means loss is equivalent to a slight change in the sampling rate.)
- The sFlow Collector can receive data from multiple switches, providing a real-time synchronized view of the whole network.
- The sFlow Collector can analyze traffic patterns for whatever protocols are found in the packet headers (for example, TCP/IP, IPX, Ethernet, AppleTalk). There is no need for the layer 2 switch to decode and understand all protocols.

Definitions

The following table describes some of the main sFlow terms and concepts.

Table 28-1 sFlow Definitions

Term	Definition
Data Source	A Data Source refers to a location within a Network Device that can make traffic measurements. Possible Data Sources include interfaces, physical entities within the device such as the backplane, and VLANs.
Packet Flow	A Packet Flow is defined as the path or trajectory that a packet takes through a Network Device (That is, the path that a packet takes as it is received on one interface, is subjected to a switching/ routing decision, and is then sent on another interface).
Packet Flow Sampling	Packet Flow Sampling refers to the random selection of a fraction of the Packet Flows observed at a Data Source.
Sampling Rate	The Sampling Rate specifies the ratio of packets observed at the Data Source to the samples generated.
Sampling Interval	The time period between successive Counter Samples.
sFlow Instance	An sFlow Instance refers to a measurement process associated with a Data Source.
sFlow Agent	The sFlow Agent provides an interface for configuring the sFlow Instances within a device.
sFlow Collector	An sFlow Collector receives sFlow Datagrams from one or more sFlow Agents. The sFlow Collector may also configure sFlow Instances using the configuration mechanisms provided by the sFlow Agent.
sFlow Datagram	An sFlow Datagram is a UDP datagram that contains the measurement data, and information about the measurement source and process.

sFlow Agent Functionality

Packet flow sampling and counter sampling are performed by sFlow Instances associated with individual Data Sources within the sFlow Agent. Packet flow sampling and counter sampling are designed as part of an integrated system. Both types of samples are combined in sFlow datagrams. Packet flow sampling will cause a steady, but random, stream of sFlow datagrams to be sent to the sFlow Collector. Counter samples may be taken opportunistically in order to fill these datagrams.

In order to perform packet flow sampling, an sFlow Sampler Instance is configured with a sampling rate. The packet flow sampling process results in the generation of packet flow records. In order to perform counter sampling, an sFlow Poller Instance is configured with a polling interval. The counter sampling process results in the generation of counter records. The sFlow Agent collects counter records and packet flow records and sends them in the form of sFlow datagrams to sFlow Collectors.

Sampling Mechanisms

Two forms of sampling are performed by the sFlow Agent: statistical packet-based sampling of switched or routed packet flows, and time-based sampling of counters.

Packet Flow Sampling

The packet flow sampling mechanism carried out by each sFlow Instance ensures that any packet observed at a Data Source has an equal chance of being sampled, irrespective of the packet flow(s) to which it belongs.

Packet flow sampling is accomplished as follows:

1. When a packet arrives on an interface, the Network Device makes a filtering decision to determine whether the packet should be dropped.
2. If the packet is not filtered (dropped), a destination interface is assigned by the switching/routing function.
3. At this point, a decision is made on whether or not to sample the packet. The mechanism involves a counter that is decremented with each packet. When the counter reaches zero a sample is taken.
4. When a sample is taken, the counter indicating how many packets to skip before taking the next sample is reset. The value of the counter is set to a random integer where the sequence of random integers used over time is the Sampling Rate.

Packet flow sampling results in the generation of Packet Flow Records. A Packet Flow Record contains information about the attributes of a packet flow, including:

- Information on the packet itself — a packet header, packet length, and packet encapsulation.
- Information about the path the packet took through the device, including information relating to the selection of the forwarding path.

Counter Sampling

The primary objective of the counter sampling is to, in an efficient way, periodically export counters associated with Data Sources. A maximum sampling interval is assigned to each sFlow Instance associated with a Data Source.

Counter sampling is accomplished as follows:

1. The sFlow Agent keep a list of counter sources being sampled.
2. When a Packet Flow Sample is generated, the sFlow Agent examines the list of counter sources and adds counters to the sample datagram, least recently sampled first.

   Counters are only added to the datagram if the sources are within a short period, 5 seconds say, of failing to meet the required sampling interval.
3. Periodically, say every second, the sFlow Agent examines the list of counter sources and sends any counters that need to be sent to meet the sampling interval requirement.

The set of counters is a fixed set defined in Section 5 of the document entitled “sFlow Version 5” available from sFlow.org (http://www.sflow.org).

Usage Notes

Although the switch hardware has the capability to sample packets on any port, to ensure that CPU utilitization is not compromised, the number of sFlow samplers that can be configured per switch or stack of switches is limited to a maximum of 32. There is no limitation on the number of pollers that can be configured.

Under certain circumstances, the switch will drop packet samples that the sFlow implementation is not able to count and therefore cannot correctly report sample_pool and drops fields of flow samples sent to the sFlow Collector. Under heavy load, this sample loss could be significant and could therefore affect the accuracy of the sampling analysis.

sFlow is disabled by default on SecureStack and G-Series devices.

Example Configuration

The general procedure for configuring sFlow includes:

1. Configure your sFlow Collector information to be used by the sFlow Agent on the switch. Up to eight Collectors can be configured. The information is stored in the sFlowReceiverTable.
2. Enable and configure sFlow packet flow sampling instances on each port.
3. Enable and configure sFlow counter sampling poller instances on each port.

The following is an example of the commands used to configure sFlow:

```
# configure sFlow Collector 1
# accept defaults for datagram size and port
set sflow receiver 1 owner enterasys timeout 180000
set sflow receiver 1 ip 192.168.16.91
#
#configure packet sampling instances on ports 1 through 12
#assign to sFlow Collector 1
set sflow port ge.1.1-12 sampler 1
set sflow port ge.1.1-12 sampler maxheadersize 256
set sflow port ge.1.1-12 sampler rate 2048
#
#configure counter poller instances on ports 1 through 12
#assign to sFlow Collector 1
set sflow port ge.1.1-12 poller 1
set sflow port ge.1.1-12 poller interval 20
```

Commands

show sflow receivers

Use this command to display the contents of the sFlow Receivers Table, or to display information about a specific sFlow Collector listed in the table.

Syntax

show sflow receivers [*index*]

Parameters

index	(Optional) Specifies a specific Collector to display information about.

Defaults

The contents of the sFlow Receivers Table is displayed.

Mode

Switch command, read-only.

Usage

Executing this command without specifying an index into the sFlow Receivers Table displays information about all the Collectors configured on the switch.

If you specify an individual Collector by its index number, additional information is displayed for that Collector.

Examples

This example displays the sFlow Receivers Table.

```
C3(su)->show sflow receivers
Receiver Owner    Time out   Max Datagram Port  IP Address
 Index    String              Size
 -------- -------- ---------- ------------ ----- ------------------
 1        ets1     17766      1400         6343  10.1.2.117
 2                 0          1400         6343  0.0.0.0
 3                 0          1400         6343  0.0.0.0
 4                 0          1400         6343  0.0.0.0
 5                 0          1400         6343  0.0.0.0
 6                 0          1400         6343  0.0.0.0
 7                 0          1400         6343  0.0.0.0
 8                 0          1400         6343  0.0.0.0
```

This example displays information about the Collector with index 1.

```
C3(su)->show sflow receivers 1
Receiver Index                          1
Owner String                            ets1
Time out                                17758
IP Address:                             10.1.2.117
Address Type                            IPv4
Port                                    6343
Datagram Version                        5
Maximum Datagram Size                   1400
```

The following table describes the output fields.

Table 28-2 show sflow receivers Output Descriptions

Output...	What it displays...
Receiver Index	Index number of a specific Collector entry in the sFlow Receivers Table. Up to 8 Collectors may be configured.
Owner String	Identity string of the Collector. An empty string indicates that the entry is unclaimed and cannot be assigned to a sampler or poller instance. The owner string is configured with the set sflow receiver owner command.
Time Out	The time remaining, in seconds, before the sampler or poller is released and stops sending samples to this receiver/Collector. The timeout value is configured with the set sflow receiver owner command.
IP Address	The IP address of this receiver/Collector. The IP address is configured with the set sflow receiver ip command.
Address Type	Whether the Collector IP address is IPv4 or IPv6.
Port	The UDP port number on this receiver/Collector to which sample datagrams should be sent. The default value is 6343, which can be changed with the set sflow receiver port command.
Datagram Version	Specifies the sFlow version used for formatting the sample datagrams.
Max Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram to this receiver/Collector. The default value is 1400 bytes, which can be changed with the set sflow receiver maxdatagram command.

set sflow receiver owner

Use this command to configure the owner identity string and timeout value for an sFlow Collector in the switch's sFlow Receivers Table.

Syntax

set sflow receiver *index* **owner** *owner-string* **timeout** *timeout*

Parameters

index	Index number in the sFlow Receivers Table for the receiver/Collector being configured. The *index* can range from 1 to 8.
owner *owner-string*	The identity string of the receiver/Collector being configured. The string can be up to 127 characters in length.
timeout *timeout*	The time, in seconds, remaining before the receiver/Collector being configured and all associated samplers and pollers expire. The value can range from 0 to 4294967295 seconds.

Defaults

None.

Mode

Switch command, read-write.

Usage

In order for an sFlow Collector to be assigned to receive sample datagrams from the sFlow Agent on the switch, an entry for that Collector must be configured in the switch's sFlow Receivers Table. An entry must contain an owner identity string, a non-zero timeout value, and the IP address of the Collector. Configure the IP address with the set sflow receiver ip command.

An entry without an owner identity string is considered unclaimed and cannot be assigned as a receiver to sampler or poller instances.

Once the timer set by this command expires, the receiver/Collector and all the samplers and pollers associated with this Collector expire and are removed from the switch's configuration. In order to start sending sample data to the Collector again, the Collector must be reconfigured with a new timeout value and samplers and pollers must be configured again. Therefore, you should consider setting the timeout value to the largest value that is reasonable for your environment.

Example

This example configures an entry for index 1 in the sFlow Receivers Table.

```
C3(su)->set sflow receiver 1 owner ets1 timeout 180000
```

set sflow receiver ip

Use this command to configure the IP address of an sFlow Collector in the switch's sFlow Receivers Table.

Syntax

set sflow receiver *index* **ip** *ipaddr*

Parameters

index	Index number in the sFlow Receivers Table for the receiver/Collector being configured. The *index* can range from 1 to 8.
ip *ipaddr*	The IP address of the receiver/Collector being configured. An IP address of 0.0.0.0 means that no sample datagrams will be sent to the Collector.

Defaults

The default IP address is 0.0.0.0.

Mode

Switch command, read-write.

Usage

In order for an sFlow Collector to be assigned to receive sample datagrams from the sFlow Agent on the switch, an entry for that Collector must be configured in the switch's sFlow Receivers Table. An entry must contain an owner identity string, a non-zero timeout value, and the IP address of the Collector. Configure the owner identity string and timeout value with the set sflow receiver owner command.

Sample datagrams will not be sent to a Collector whose entry in the sFlow Receivers Table has an IP address of 0.0.0.0.

Example

This example configures an IP address of 10.10.10.10 to index entry 1.

```
C3(su)->set sflow receiver 1 ip 10.10.10.10
```

set sflow receiver maxdatagram

Use this command to set the maximum number of data bytes that can be sent in a single sample datagram.

Syntax

set sflow receiver *index* **maxdatagram** *bytes*

Parameters

index	Index number in the sFlow Receivers Table for the receiver/Collector being configured. The *index* can range from 1 to 8.
maxdatagram *bytes*	Specifies the maximum number of data bytes that can be sent in a single sample datagram. This size should be set to avoid fragmentation of the sFlow datagrams. The value of *bytes* can range from 200 to 9116. The default is 1400.

Defaults

Default maximum datagram size is 1400 bytes.

Mode

Switch command, read-write.

Example

This example sets the maximum datagram size to 2800 bytes for index entry 1.

```
C3(su)->set sflow receiver 1 maxdatagram 2800
```

set sflow receiver port

Use this command to configure the UDP port on the sFlow Controller to which the switch will send sample datagrams.

Syntax

set sflow receiver *index* **port** *port*

Parameters

index	Index number in the sFlow Receivers Table for the receiver/Collector being configured. The *index* can range from 1 to 8.
port *port*	Specifies the UDP port on the receiver/Collector to which the sample datagrams should be sent. By default, the port is 6343.

Defaults

The default port value is 6343.

Mode

Switch command, read-write.

Example

This example changes the sFlow receiver port on the Collector to 1234.

```
C3(su)->set sflow receiver 1 port 1234
```

clear sflow receiver

Use this command to delete a receiver/Collector from the sFlow Receivers Table, or to return certain parameters to their default values for the specified Collector.

Syntax

clear sflow receiver *index* [**ip** | **maxdatagram** | **owner** [**timeout**] | **port**]

Parameters

index	Index number in the sFlow Receivers Table for the receiver/Collector being configured. The *index* can range from 1 to 8.
ip	(Optional) Clear the IP address to 0.0.0.0. Sample datagrams are not sent to Collectors with an IP address of 0.0.0.0.
maxdatagram	(Optional) Return the maximum datagram size to 1400 bytes.

owner	(Optional) Clear the owner identity string. Entries in the sFlow Receiver Table without an identity string are considered unclaimed.
timeout	(Optional) Clear the timeout value of the specified entry.
port *port*	(Optional) Clear the UDP port on the receiver/Collector to which the sample datagrams should be sent. The value is reset to the default of 6343.

Defaults

If no optional parameters are specified, the entire entry is cleared.

Mode

Switch command, read-write.

Usage

You can clear the IP address, maximum datagram size, or UDP port without deleting an entry from the sFlow Receivers Table. If you clear the owner or timeout, the entire entry is cleared. If you enter only an entry index and none of the optional parameters, the entire entry is cleared.

Once an entry is cleared, all pollers and samplers associated with that receiver are also removed from the switch configuration.

Example

This example returns the maximum datagram size to the default of 1400 bytes for the Collector with index 1.

```
C3(su)->clear sflow receiver 1 maxdatagram
```

set sflow port poller

Use this command to configure poller instances on ports, or data sources.

Syntax

set sflow port *port-string* **poller** {*index* | **interval** *seconds*}

Parameters

port-string	Specifies the port or ports (data sources) on which the poller instance is being configured.
index	Index number in the sFlow Receivers Table for the receiver/Collector with which the poller instance is associated. The *index* can range from 1 to 8.
interval *seconds*	Specifies the polling interval, which can range from 0 to 86400 seconds. A value of 0 disables counter sampling.

Defaults

The default interval value is 0 seconds, which disables counter sampling.

Mode

Switch command, read-write.

Usage

A poller instance performs counter sampling on the data source to which it is configured. Refer to "Sampling Mechanisms" on page 28-2 for more information.

You must first associate a receiver/Collector in the sFlow Receivers Table with the poller instance, before configuring the polling interval.

When a receiver times out or is cleared from the sFlow Receivers Table, all poller and sampler instances associated with that receiver are also cleared from the switch's configuration.

Example

The following example configures poller instances on ports ge.1.1 through ge.1.8 and associates them with receiver 1. Then, a polling interval of 240 seconds is configured.

```
C3(su)->set sflow port ge.1.1-8 poller 1
C3(su)->set sflow port ge.1.1-8 poller interval 240
```

show sflow pollers

Use this command to display information about configured poller instances.

Syntax

`show sflow pollers`

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example displays the output of this command.

```
C3(su)->show sflow pollers
 Poller        Receiver  Poller
 Data Source   Index     Interval
 -----------   -------   -------
 ge.1.1        1         240
 ge.1.2        1         240
 ge.1.3        1         240
 ge.1.4        1         240
 ge.1.5        1         240
 ge.1.6        1         240
 ge.1.7        1         240
 ge.1.8        1         240
```

clear sflow port poller

Use this command to change the poller interval or to remove poller instances.

Syntax

clear sflow port *port-string* **poller** [**interval**]

Parameters

port-string	Specifies the port or ports on which the poller instance is being cleared.
interval	(Optional) Specifies that the polling interval should be cleared to 0. A value of 0 disables counter sampling.

Defaults

If **interval** is not specified, the poller instance is cleared.

Mode

Switch command, read-write.

Example

This example removes the poller instance on port ge.1.1.

```
C3(su)->clear sflow port ge.1.1 poller
```

set sflow port sampler

Use this command to configure sampler instances on ports, or data sources.

Syntax

set sflow port *port-string* **sampler** {*index* | **maxheadersize** *bytes* | **rate** *rate*}

Parameters

port-string	Specifies the port or ports (data sources) on which the sampler instance is being configured.
index	Index number in the sFlow Receivers Table for the receiver/Collector with which the sampler instance is associated. The *index* can range from 1 to 8.
maxheadersize *bytes*	Specifies the maximum number of bytes that should be copied from the sampler packet. The value can range from 20 to 256 bytes. The default is 128 bytes.
rate *rate*	Specifies the statistical sampling rate for sampling from this data source. The value of *rate* specifies the number of incoming packets from which one packet will be sampled. For example, if the rate is 1024, one packet will be sampled from every 1024 ingressing packets on this data source. The rate can range from 1024 to 65536. A value of 0 disables sampling. The default value is 0.

Defaults

None.

Mode

Switch command, read-write.

Usage

A sampler instance performs packet flow sampling on the data source to which it is configured. Refer to "Sampling Mechanisms" on page 28-2 for more information.

You must first associate a receiver/Collector in the sFlow Receivers Table with the sampler instance, before configuring the sampling rate or maximum number of bytes copied from sampled packets.

When a receiver times out or is cleared from the sFlow Receivers Table, all poller and sampler instances associated with that receiver are also cleared from the switch's configuration.

A maximum of 32 sampler instances can be configured per switch or stack of switches.

Example

The following example configures sampler instances on ports ge.1.1 through ge.1.8 and associates them with receiver 1. Then, a sampling rate of 1024 is configured. The default max header size of 128 bytes is used.

```
C3(su)->set sflow port ge.1.1-8 sampler 1
C3(su)->set sflow port ge.1.1-8 sampler rate 1024
```

show sflow samplers

Use this command to display information about configured sampler instances.

Syntax

show sflow samplers

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example displays the output of this command.

```
C3(su)->show sflow samplers
 Sampler      Receiver  Packet          Max Header
 Data Source  Index     Sampling Rate   Size
 -----------  -------   -------------   ----------
 ge.1.1       1         1024            128
```

```
ge.1.2      1       1024          128
ge.1.3      1       1024          128
ge.1.4      1       1024          128
ge.1.5      1       1024          128
ge.1.6      1       1024          128
ge.1.7      1       1024          128
ge.1.8      1       1024          128
```

clear sflow port sampler

Use this command to change the sampler rate or maximum header size, or to remove sampler instances.

Syntax

clear sflow port *port-string* **sampler** [**maxheadersize** | **rate**]

Parameters

port-string	Specifies the port or ports on which the sampler instance is being cleared.
maxheadersize	(Optional) Specifies that the maximum header size should be cleared to the default value of 128 bytes.
rate	(Optional) Specifies that the sampling rate should be cleared to the default value of 0, which disables sampling by the instance.

Defaults

If neither optional parameter is specified, the sampler instance is cleared.

Mode

Switch command, read-write.

Example

This example removes the sampler instance on port ge.1.1.

```
C3(su)->clear sflow port ge.1.1 sampler
```

set sflow interface

Use this command to specify the interface used for the source IP address of the sFlow Agent when sending sampling datagrams to the sFlow Collector.

Syntax

set sflow interface {**loopback** *loop-ID* | **vlan** *vlan-ID*}

Parameters

loopback *loop-ID*	Specifies the loopback interface to be used. The value of *loop-ID* can range from 0 to 7.

vlan *vlan-ID*	Specifies the VLAN interface to be used. The value of vlan-ID can range from 1 to 4093.

Defaults

None.

Mode

Switch command, read-write.

Usage

This command allows you to configure the management interface used by the sFlow Agent when sending sampling datagrams to the sFlow Collector. Any of the interfaces, including VLAN routing interfaces, can be configured as the management interface.

An interface must have an IP address assigned to it before it can be set by this command.

If no interface is specified, then the Host VLAN will be used as the management interface.

If a non-loopback interface is configured with this command, application packet egress is restricted to that interface if the server can be reached from that interface. Otherwise, the packets are transmitted over the first available route. Packets from the application server are received on the configured interface.

If a loopback interface is configured, and there are multiple paths to the application server, the outgoing interface (gateway) is determined based on the best route lookup. Packets from the application server are then received on the sending interface. If route redundancy is required, therefore, a loopback interface should be configured.

Example

This example configures an IP address on VLAN interface 100 and then sets that interface as the management interface for the sFlow Agent.

```
C3(rw)->router(Config-if(Vlan 100))#ip address 192.168.10.1 255.255.255.0
C3(rw)->router(Config-if(Vlan 100))#exit
C3(rw)->router(Config)#exit
C3(rw)->router#exit
C3(rw)->router>exit
C3(rw)->set sflow interface vlan 100

C3(rw)->show sflow interface
vlan 100  192.168.10.1
```

show sflow interface

Use this command to display the interface used by the sFlow Agent when sending sampling datagrams to the sFlow Collector.

Syntax

```
show sflow interface
```

Parameters

None.

Defaults

None.

Mode

Switch mode, read-only.

Example

This example displays the output of this command. In this case, the IP address assigned to loopback interface 1 will be used as the source IP address of the sFlow Agent.

```
C3(rw)->show sflow interface
loopback 1  192.168.10.1
```

clear sflow interface

Use this command to clear the management interface used by the sFlow Agent back to the default of the Host VLAN.

Syntax

clear sflow interface

Parameters

None.

Defaults

None.

Mode

Switch command, read-write.

Example

This command returns the managment interface used by the sFlow Agent back to the default of the Host VLAN.

```
C3(rw)->show sflow interface
vlan 100  192.168.10.1
C3(rw)->clear sflow interface
C3(rw)->
```

show sflow agent

Use this command to display information about the sFlow Agent.

Syntax

show sflow agent

Parameters

None.

Defaults

None.

Mode

Switch command, read-only.

Example

This example displays the output of this command.

```
C3(rw)->show sflow agent
sFlow Version                                   1.3;Broadcom Corp.;06.03.00.0001T
IP Address                                       192.168.1.6
```

A

Policy and Authentication Capacities

This appendix lists the policy and authentication capacities of the SecureStack C3 as of the date this document was published. Please refer to the Release Notes for your firmware version for the latest capacity information.

Policy Capacities

Refer to the "Configuring Policy" Feature Guide for an in-depth discussion of Policy configuration. This Feature Guide is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

Table A-1 Policy Capacities

Feature	Capacity
Maximum policy roles (profiles) per system	15
Maximum number of unique rules per system	768
Maximum number of ether type rules	128
Maximum number of MAC rules	128
Maximum number of Layer 3/4 rules	512
Maximum number of rules per single role	100
Maximum number of masks	No limit
CoS rate limiting (IRL) support	Yes
Priority-based rate limiting	No
Rule-based rate limiting	No
Role-based rate limiting	Yes
Fixed rule precedence	Yes
Supported rule types	
ether type (numuser = 1)[1]	vlan/cos/drop/fwd (max 7 vlan rules per profile)
mac dest/mac source	cos/drop/fwd
ip protocol[1]	cos/drop/fwd
ip dest socket/ip source socket	cos/drop/fwd
ip tos[1]	cos/drop/fwd
tcp dest port/ tcp source port	cos/drop/fwd

Table A-1 Policy Capacities (Continued)

Feature	Capacity
udp dest port/udp source port	cos/drop/fwd
icmp type[1]	No

1. These rules cannot be masked.

Authentication Capacities

Refer to the "Configuring User Authentication" Feature Guide for an in-depth discussion of authentication configuration. This Feature Guide is located on the Enterasys Networks web site:

http://www.enterasys.com/support/manuals/

Table A-2 Authentication Capacities

Authentication Feature	Capacity
IEEE 802.1x (dot1x) authentication	Supported
MAC-based authentication	Supported
Port Web Authentication (PWA)	Supported
RFC 3580 dynamic VLAN assignment based on authentication response	Supported, for 802.1x, MAC-based, and PWA authentication methods
Multi-user authentication maximum users per port when policy maptable response is:	
policy mode	3
both, hybrid mode	3
tunnel mode	6
User + IP phone (Configured with a policy admin rule) Multiauth numusers set to 2	Supported

Index